DOCTRINE

Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel

Cécile de Terwangne[1], Karen Rosier[2] et Bénédicte Losdyck[3]

La contribution a pour objectif de donner un premier éclairage sur les grandes nouveautés qu'introduit le Règlement général sur la protection des données. Le Règlement entend renforcer les droits des personnes concernées et mieux appréhender les risques liés aux traitements qui ont évolué avec les innovations technologiques. Si les principes de base du traitement des données qu'avait introduits la directive 95/46 dans le droit de l'Union ne sont pas fondamentalement modifiés, le Règlement innove toutefois sur bien des points. Son entrée en vigueur en 2018 entraînera notamment de nouvelles obligations pour les responsables de traitement et les sous-traitants. Le texte soulève à l'heure actuelle de nombreuses interrogations quant à sa mise en œuvre. Cette première analyse se veut didactique tout en mettant en évidence des difficultés d'interprétation qui méritent réflexion.

• • •

The aim of this contribution is to shed some light on the major innovations introduced by the General Data Protection Regulation. The Regulation intends to strengthen the rights of the data subjects and to deal more adequately with the risks created by the evolving data processing practices due to technological innovations. While the key principles of data processing introduced by EU Directive 95/46 are not fundamentally amended, the Regulation innovates on many topics. Its entry into force in 2018 will entail new obligations for data controllers and processors. The text raises questions about its implementation. This first analysis aims at being didactic while highlighting difficulties of interpretation that deserve further consideration.

1 Professeur à la Faculté de droit de l'UNamur et directrice de recherche au CRIDS.
2 Maître de conférences à la Faculté de droit de l'UNamur. Chercheuse au CRIDS. Avocate.
3 Chercheuse au CRIDS. Avocate.

I. INTRODUCTION

1. Une véritable révision de la réglementation. Le moins que l'on puisse dire est que le Règlement général sur la protection des données (ci-après, le « Règlement »)[4] était attendu. Attendu, tout d'abord, parce que la directive 95/46/CE[5] (ci-après la « Directive ») qu'il remplace avait été adoptée en 1995 et n'avait pas anticipé les révolutions numériques qu'ont insufflées successivement la généralisation d'internet, le web 2.0 et le grand dévoilement sur les réseaux sociaux, le cloud et le *big data* notamment. La collecte, le partage et le transfert de données à caractère personnel s'en sont trouvés dopés et de nouveaux enjeux de société ont mis en évidence tant l'importance de pouvoir traiter les données que la nécessité d'une protection en adéquation avec la réalité technologique advenue.

Le Règlement s'est également fait attendre puisque la proposition de Règlement était sur la table depuis janvier 2012 et était elle-même le fruit de larges et longues concertations sur la réforme de la Directive en chantier depuis plusieurs années.

Le résultat est ambitieux. Il s'agit, sur bien des points, d'une réforme qui n'a rien de cosmétique. Notre propos est de dégager les principales nouveautés et les premiers commentaires que suscitent ces nouveautés.

2. Un contexte de révision des instruments internationaux de la protection des données. Avant d'entamer ces développements, il convient de signaler que la réforme de la Directive qui se dessinait dans le contexte de l'Union européenne s'est inscrite dans une réflexion globale de révision des instruments de protection des données. Ainsi, les travaux de modernisation de la Convention 108 du Conseil de l'Europe relative à la protection des personnes à l'égard des traitements de données à caractère personnel ont démarré dès 2010, et les Lignes directrices de l'OCDE en la matière ont été soumises à un même processus de révision qui a abouti le 11 juillet 2013 à l'adoption de nouvelles « Privacy Guidelines »[6]. Il est à noter que sur plusieurs points, les discussions menées à Strasbourg et Bruxelles ont pu conduire à un enrichissement commun dans l'exercice de modernisation des deux instruments européens. Un grand souci de cohérence entre les deux textes a d'ailleurs animé les acteurs de la réforme car il était impératif pour les États membres de l'Union européenne signataires de la Convention 108 de ne pas être confrontés à des exigences contradictoires.

3. L'occasion d'affirmer le droit à la protection des données comme un droit autonome. Le Règlement entend par ailleurs s'ancrer directement dans le droit à la protection des données à caractère personnel[7], sans doute dans l'optique de promouvoir l'autonomie de ce droit par rapport au droit au respect de la vie privée. On ne fait plus référence dans les dispositions introductives du Règlement à la protection de la vie privée. L'article 1er du Règlement précise de façon plus générale que « Le présent règlement protège les libertés et droits fonda-

4 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

5 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

6 OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (2013), C(80)58/FINAL, telles qu'amendées le 11 juillet 2013 par C(2013)79, www.oecd.org.

7 Ce droit a été consacré séparément du droit au respect de la vie privée à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

mentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel ». Cette formulation doit toutefois être bien comprise : le Règlement n'a bien sûr pas vocation à protéger les libertés et droits fondamentaux des personnes physiques de manière générale, mais bien dans le contexte du traitement de données à caractère personnel. Le considérant 4 du Règlement souligne par ailleurs que la protection des données à caractère personnel n'est pas un droit absolu et doit être considérée par rapport à sa fonction dans la société et être mise en balance avec les libertés et autres droits fondamentaux, conformément au principe de proportionnalité.

II. LE MODE RÉGULATOIRE REVU ET CORRIGÉ

4. Pourquoi un règlement plutôt qu'une directive ? L'une des critiques formulées à propos de la Directive était l'échec d'une véritable harmonisation de la réglementation. La raison en était de trop grandes divergences entre les législations nationales au terme de l'exercice de transposition de la Directive par les États membres. Il est évident que dans des marchés qui dépassent le plus souvent les frontières, la coexistence de législations nationales prévoyant des conditions de traitement différentes d'un pays à l'autre est un frein à la construction de *business models* internationaux. Le choix d'un règlement comme instrument de régulation devrait lever cet obstacle puisque le texte s'appliquera tel quel dans tous les États membres à dater du 25 mai 2018, date à laquelle la Directive sera abrogée. Les traitements en cours avant l'entrée en vigueur du Règlement doivent être mis en conformité avec celui-ci pour cette échéance[8].

Le Règlement entend faire œuvre de cohérence dans les règles applicables avec pour objectifs non seulement d'assurer la libre circulation des données au sein de l'Union mais également un haut niveau de protection des données homogène d'un État à l'autre. Il est également question de renforcer l'effectivité de cette protection pour restaurer un meilleur niveau de confiance des consommateurs, en particulier dans l'environnement numérique[9].

5. Articulation du Règlement avec d'autres directives. Il convient toutefois de noter d'emblée que le Règlement ne sera pas le seul instrument voué à régir la protection des données au niveau européen. Outre le règlement 45/2001[10] qui reste d'application, des traitements seront régis par d'autres textes européens.

Pour les traitements réalisés dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union, le Règlement[11] n'impose pas d'obligations supplémentaires aux acteurs pour les aspects pour lesquels ils sont déjà soumis à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE[12]. Le considérant 173 précise toutefois que le Règlement s'appliquera à tous les autres aspects. La cohabitation des deux régimes n'est cependant pas aisée à appréhender dès lors qu'il faudrait pouvoir identifier quels sont les objec-

8 Article 99, § 2, du Règlement.

9 *Cfr* considérant 10 du Règlement.

10 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

11 Article 95 du Règlement.

12 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

tifs communs poursuivis et comment ils sont rencontrés dans chacun des deux textes. Afin d'éviter toute redondance ou contradiction avec le Règlement, la directive 2002/58/CE est actuellement soumise à révision.

Par ailleurs, en marge du Règlement, la directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données a été adoptée le 27 avril 2016[13]. Cette directive établit des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation des données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière. Elle devra être transposée par les États membres en droit interne pour le 6 mai 2018.

6. La voie ouverte à une inflation des règles en matière de protection des données. Une singularité du Règlement qui saute immédiatement aux yeux du praticien est sa longueur : 99 articles et pas moins de 173 considérants. Le texte, largement inspiré de celui de la Directive, devient plus exhaustif pour apporter des précisions là où des lacunes avaient suscité ou pourraient susciter des discussions ou pour définir de nouveaux concepts et développer de nouvelles règles, ou encore intégrer des règles qui ne sont pas neuves dès lors qu'elles s'inspirent du travail de la Commission européenne et du Groupe de l'article 29 (concernant les règles contraignantes d'entreprise en matière de flux transfrontières de données, notamment). Cet effort d'exhaustivité n'est toutefois pas gage d'élimination de toute difficulté d'interprétation. En témoignent déjà les premières observations quant aux divergences terminologiques dans les traductions du Règlement[14].

Par ailleurs, il est à noter que le texte du Règlement est voué à être complété par d'autres textes. La Commission européenne se voit conférer un pouvoir d'exécution lui permettant d'adopter des règles directement applicables, par le biais d'actes délégués ou d'exécution, dans des domaines précis (par exemple, concernant le nouveau droit à la portabilité des données que nous évoquerons *infra*). L'adoption de textes par la Commission n'est pas un phénomène nouveau en la matière puisqu'on connaît les décisions de la Commission en matière d'adéquation concernant des pays tiers à l'Espace économique européen et les clauses contractuelles-types pour les flux transfrontières. Les apports de la Commission sont toutefois appelés à se multiplier au vu des attributions nouvelles concernant la définition d'icônes normalisées pour la communication d'informations aux personnes concernées[15] ou encore le processus de certification des responsables du traitement[16], notamment[17]. Il est toutefois à noter que les aspects de la réglementation sur lesquels la Commission est habilitée à intervenir ont été considérablement réduits par rapport à la proposition de règlement initiale. L'étendue du pouvoir laissé

13 Directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.*, L 119, 4 mai 2016, pp. 89-131.

14 Voy. les exemples épinglés ponctuellement dans le cadre de cette contribution, *infra*.

15 Article 12, §§ 8 et 92, du Règlement.

16 Article 43, §§ 9 et 92, du Règlement.

17 La Commission dispose également de compétences d'exécution notamment en matière de flux transfrontières (art. 45 et 46), de sous-traitance (art. 28, § 7), de codes de conduite (art. 40), de règles d'entreprises contraignantes (art. 47 du Règlement).

à la Commission avait d'ailleurs fait l'objet de vives critiques, non seulement car il n'était pas cantonné à des éléments non essentiels de la réglementation comme requis par l'article 290, paragraphe 1er, du TFUE qui prévoit ce mécanisme[18], mais également car il rendait l'applicabilité du Règlement trop dépendante de l'adoption de ces actes au vu de l'importance des points qui étaient voués à être réglés par la Commission[19].

En marge de la réglementation, un Comité européen de la protection des données, qui remplacera le Groupe de l'article 29, est créé et aura notamment pour mission de publier des lignes directrices, des recommandations et des bonnes pratiques concernant différents aspects de la protection des données[20]. Pour assurer la transition vers le nouveau régime, le Groupe de l'article 29 a annoncé une série de mesures qu'il comptait prendre, en ce compris des lignes directrices sur certains aspects du Règlement[21]. Au moment d'écrire ces lignes, le Groupe de l'article 29 n'avait pas encore publié ses Guidelines.

7. Le Règlement : un texte par et pour des spécialistes ? L'inflation de règles et de directives plus précises et complètes devrait permettre d'assurer une meilleure homogénéité dans la protection des données mais le risque de cette évolution est que la matière de la protection des données devienne plus que jamais affaire de spécialistes. Or, comme on le verra, le Règlement vise clairement à responsabiliser davantage les responsables du traitement en exigeant d'eux anticipation et gestion des risques en matière de protection des données, tout en durcissant les sanctions en cas de manquement au Règlement. Cela suppose une bonne compréhension de la réglementation qui, il faut l'avouer, était surtout jusqu'à aujourd'hui l'apanage des grandes entreprises et administrations disposant d'un service juridique averti. Nous verrons que le Règlement tente de pallier ce possible décalage en mettant en place divers mécanismes.

Nous identifions deux grandes tendances à cet égard. D'une part, il s'agit d'instaurer l'obligation pour le responsable du traitement de recourir à des spécialistes dans certains cas de figure (on pense à l'obligation de désignation par le responsable du traitement et le sous-traitant d'un délégué à la protection des données justifiant de connaissances spécialisées en la matière[22], ou encore à l'obligation de procéder à une analyse d'impact dans certains cas préalablement à la mise en œuvre d'un traitement qui sera bien souvent elle aussi réalisée par une entreprise spécialisée). D'autre part, le Règlement appelle la mise en place d'outils de « standardisation » de la protection des données via l'établissement de contrats-types par la Commission – pour les transferts de données mais également pour la sous-traitance –, la promotion de codes de conduite, l'encadrement de mécanismes de certification, la définition d'icônes normalisées pour une information simplifiée vis-à-vis des personnes concernées, pour ne citer que ces exemples.

8. Les limites de l'harmonisation entre législations nationales. Toute disparité entre les législations nationales n'est par ailleurs pas éliminée. En effet, le Règlement maintient pour les États un pouvoir de prévoir des règles spéci-

18 Avis du Contrôleur européen de la protection des données sur le paquet de mesures pour une réforme de la protection des données, 7 mars 2012, www.edps.europa.eu, p. 14.

19 C. Gayrel et R. Robert, « Proposition de règlement sur la protection des données. Premiers commentaires », *J.D.E.*, 2012, p. 181.

20 Voy. articles 68 et 70 du Règlement.

21 Groupe de l'article 29, « Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR) », WP 236, 2 février 2016.

22 Articles 37 et suivants du Règlement.

fiques (i) pour des traitements qui poursuivent certaines finalités, (ii) qui portent sur certaines catégories de données, (iii) qui concernent certaines catégories de personnes, ou encore (iv) qui ont trait à certaines problématiques appelant un arbitrage des intérêts en présence sur lequel un consensus au niveau européen n'a pas pu ou voulu être réalisé.

i. Dérogations liées à des finalités spécifiques. Ainsi le Règlement conserve-t-il tout d'abord aux États membres une possibilité d'adopter des exigences spécifiques à respecter pour des traitements découlant d'obligations légales ou pour ceux qui interviennent dans le cadre d'une mission d'intérêt public ou qui relèvent de l'exercice de l'autorité publique dont est investi le responsable du traitement[23]. Cela permet de conserver en Belgique des législations sectorielles parallèles à la loi du 8 décembre 1992 pour autant qu'elles soient conformes au nouveau Règlement. On pense, par exemple, aux réglementations sur les banques-carrefour.

ii. Dérogations liées à certaines catégories de données. Les États membres peuvent prévoir des conditions ou limitations supplémentaires par rapport à ce qui est arrêté par le Règlement en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé[24]. Le Règlement réintroduit en réalité des possibilités de dérogations dans les règles harmonisées. Le considérant 53 du Règlement indique toutefois de manière laconique que « cette possibilité ne devrait pas entraver le libre flux des données à caractère personnel au sein de l'Union lorsque ces conditions s'appliquent au traitement transfrontalier de ces données ». Le concept de traitement transfrontalier défini à l'article 4, 23), du Règlement concerne un traitement qui est effectué sur plusieurs territoires ou qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres. On n'aperçoit pas immédiatement ce qu'implique la précision du considérant : les États membres ne pourraient prévoir des dérogations qui fassent obstacle à un flux de données vers un autre État membre lorsqu'il est question d'un traitement transfrontalier ? Ou faut-il comprendre que de telles dérogations peuvent être prévues mais devraient être levées lorsqu'il est question de traitement transfrontalier ? La question sera d'autant plus complexe lorsqu'on aura affaire à des traitements se déroulant sur plusieurs territoires avec des lois nationales applicables dont les critères de rattachement ne sont plus évoqués dans le Règlement[25]. Il peut donc être théoriquement question de plusieurs lois nationales s'appliquant à un traitement transfrontalier sans qu'un critère ne donne priorité à l'une ou l'autre loi nationale applicable.

iii. Dérogations liées à certaines catégories de personnes concernées. Les États membres peuvent également adopter des règles spécifiques au traitement des données à caractère personnel des personnes décédées, ces données n'entrant pas dans le champ d'application du Règlement[26]. Ils sont par ailleurs habilités à abaisser l'âge à partir duquel le traitement des données d'un mineur peut normalement être effectué licitement sans le consentement de son représentant légal (celui-ci est de 16 ans et ne peut être abaissé en deçà de 13 ans)[27].

iv. Dérogations liées à des arbitrages laissés aux États membres. De possibilité de limitation de certains droits, il est également encore largement question à l'article 23 du Règlement. Cette disposition prévoit la possibilité pour les

23 Article 6, § 2, du Règlement.
24 Article 9, § 4, du Règlement.
25 Voy. à ce sujet point 12, *infra*.
26 Considérant 27 du Règlement.
27 Article 8, § 1er, du Règlement et *infra*, n° 73.

États membres de limiter la portée de certains droits de la personne concernée et des obligations vis-à-vis d'elle lorsque cela se justifie au regard d'objectifs importants. On vise notamment les obligations d'information et le droit d'accès de la personne concernée, mais également l'obligation de lui notifier une violation de ses données personnelles. Les objectifs permettant de justifier des dérogations sont plus étendus que dans la Directive (et incluront désormais, par exemple, la protection de l'indépendance de la justice et des procédures judiciaires et l'exécution des demandes de droit civil). À noter une autre nouveauté : si les dérogations doivent toujours résulter d'une mesure législative, le Règlement imposera que le texte adopté contienne des spécifications minimum concernant des aspects du traitement, spécifications dont certaines sont assez classiques (les finalités du traitement ou des catégories de traitement, les catégories de données à caractère personnel, l'étendue des limitations introduites, etc.), et d'autres plus novatrices (les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites, ou encore les risques pour les droits et libertés des personnes concernées, ce dernier point ne manquant pas de poser question quant à la manière dont il pourra être mis en œuvre dans une loi).

Par ailleurs, le Règlement réserve aux États membres le soin de légiférer dans certains domaines. Nous en épinglerons deux[28]. Le premier est la conciliation de la liberté d'expression et d'information et du droit à la protection des données à caractère personnel[29]. Les exceptions liées aux fins de journalisme ou d'expression artistique ou littéraire que la Directive permettait aux États membres de prévoir ne sont pas définies dans le Règlement mais devront l'être par les États membres, dans leur droit national. Il est également question plus largement de la « liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire »[30]. Voilà donc un arbitrage épineux qui revient aux États membres et qui va diverger d'un État à l'autre à l'heure où l'on a pu mesurer la complexité de la problématique, notamment à l'occasion de la diffusion de données à caractère personnel en ligne[31].

Le second est celui du traitement des données à caractère personnel dans les relations de travail[32]. On doit concéder qu'en Belgique, le terrain est peu investi. Mises à part quelques conventions collectives de travail[33] et quelques dispositions spécifiques noyées dans des réglementations plus larges (concernant la médecine du travail, par exemple), les questions du traitement des données dans les relations de

28 Voy. également, les articles 86 et suivants qui prévoient la possibilité d'une réglementation nationale concernant le traitement et l'accès du public aux documents officiels, le traitement du numéro d'identification national, les garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, le maintien de règles existantes des églises et associations religieuses en matière de protection des données ou encore la conciliation entre les pouvoirs d'investigation des autorités de contrôle (telle la Commission de la protection de la vie privée en Belgique) et les règles de secret professionnel qui feraient obstacle à l'exercice de ce pouvoir.

29 Considérants 65 et 153 du Règlement.

30 Article 85 et considérant 153 du Règlement. On notera l'apparition d'une nouvelle notion : l'« expression universitaire » qui méritera d'être éclairée et délimitée.

31 C.J.C.E., 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy*, *Satamedia Oy*, aff. C73/07. Voy. C. de Terwangne, « Les dérogations à la protection des données en faveur des activités de journalisme enfin élucidées », note sous C.J.C.E. (gr. ch.), 16 décembre 2008, *Satakunnan Markkinapörssi Oy*, *Satamedia Oy*, aff. C-73/07, *R.D.T.I.*, 2010, n° 38, pp. 132-146.

32 Article 88 et considérant 155 du règlement.

33 En matière de cybersurveillance (CCT n° 81), de vidéo surveillance (CCT n° 68) ou encore de contrôle de la consommation de drogue ou d'alcool (CCT n° 100).

travail ne font pas l'objet d'une réglementation spécifique. Cela pourrait être appelé à évoluer.

Notons encore que les États membres gardent la main tout d'abord sur tout ce qui touche aux traitements effectués aux fins d'assurer la sécurité nationale et la sûreté de l'État. Jusqu'à présent, en droit belge, ces traitements étaient soumis à la loi du 8 décembre 1992, avec certes des exceptions partielles pour l'application de certaines dispositions[34]. Si la loi, tout comme son arrêté royal d'exécution du 13 février 2001[35], ne seront plus d'application pour la majorité des traitements et pourraient être abrogés concomitamment à l'entrée en application du Règlement, il demeure qu'il faudra prévoir une législation particulière pour ces traitements. Il en sera également ainsi pour les traitements des données à caractère personnel mis en œuvre par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces dans le cadre de la transposition de la directive 2016/680. À l'heure actuelle, on ignore encore si la loi du 8 décembre 1992 sera modifiée ou abrogée pour être remplacée par de nouveaux textes.

III. CHAMP D'APPLICATION

A. Champ d'application matériel

9. Du nouveau concernant la notion de « personne identifiable ». Le champ d'application matériel de la réglementation n'est pas formellement modifié par rapport à ce que prévoyait la Directive. Le Règlement est applicable à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

La définition de la notion-clé de « donnée à caractère personnel » intègre de nouvelles références à des moyens plus actuels qui permettent l'identification des personnes concernées, tels que le recours à des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à l'identité génétique. L'idée est de rester technologiquement neutre tout en clarifiant certains points qui ont posé question.

Point notable, le considérant 26 du Règlement affirme que le ciblage (très utilisé dans la publicité comportementale en ligne, par exemple) peut constituer une manière d'identifier directement ou indirectement une personne physique[36]. Pour être considérées comme étant relatives à une personne identifiable, il suffit donc que les données soient associées à un identifiant unique sans pour autant que le responsable du traitement dispose ou puisse disposer de données nominatives[37]. On opère donc un glissement de la notion d'identification vers un concept d'individualisation (la version anglaise utilise le terme « *singling out* », soit l'individualisation ou le ciblage).

10. Quelques variations terminologiques. Pour le reste, on relèvera que le texte français du Règlement diffère sur quelques points

34 Article 3 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.

35 Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001.

36 Voy. la position développée en ce sens par le Groupe de l'article 29 dans l'avis 16/2011 du 8 décembre 2011 sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne (p. 8), et C. Gayrel et R. Robert, « Proposition de règlement sur la protection des données. Premiers commentaires », *J.D.E.*, 2012, p. 175.

37 Considérant 26 du Règlement.

précis de celui de la Directive alors que la version anglaise le reprend tel quel. Il est désormais question, à propos de la notion de « données à caractère personnel », de données « se rapportant » à une personne physique identifiée ou identifiable au lieu de « concernant » ces personnes, là où la terminologie anglaise reste inchangée (« *relating to* »). Cela ne devrait donc pas avoir d'incidence sur la portée de la notion.

On constate le même phénomène à propos de l'exclusion du champ d'application matériel de la réglementation de traitements effectués à des fins personnelles et domestiques[38]. Il est désormais question d'activités « strictement » personnelles ou domestiques alors que la Directive visait les activités « exclusivement » personnelles ou domestiques et que le texte en anglais « *a purely personal or household activity* » est repris tel quel dans le Règlement. La portée de l'exclusion ne devrait donc pas être modifiée.

11. Les réseaux sociaux et la notion d'activité strictement personnelle ou domestique. Reste un élément interpellant que nous ne pouvons omettre de souligner. Le considérant 18 du Règlement précise que ce dernier « ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques ».

Ce texte laisse entendre que lorsqu'une personne utilise les réseaux sociaux pour correspondre, par exemple, avec des tiers (sans autre précision sur le type de profil concerné fermé/accessible au public) et qu'il ne s'agit pas d'une activité professionnelle ou commerciale, le Règlement ne s'appliquera pas à l'auteur des communications mais exclusivement aux fournisseurs du service du réseau social. Il convient de rester prudent quant à la manière dont ce considérant peut être interprété. La jurisprudence de la C.J.U.E. sur la portée de l'exclusion à des fins personnelles ou domestiques s'est prononcée pour une interprétation stricte de l'exclusion[39]. Elle a considéré dans une affaire *Frantisek Rynes*[40] que dès lors qu'une activité (en l'occurrence, une utilisation de caméra de vidéosurveillance pour protéger un domicile privé) « s'étend, même partiellement, à l'espace public et, de ce fait, est dirigée vers l'extérieur de la sphère privée de celui qui procède au traitement des données par ce moyen, elle ne saurait être considérée comme une activité exclusivement "personnelle ou domestique", au sens de l'article 3, paragraphe 2, second tiret, de la directive 95/46 ». Dans le même sens, la Cour avait déjà souligné dans l'arrêt *Lindqvist*[41] et dans l'arrêt *Satamedia*[42] que la diffusion de

38 Article 2, § 2, c), du Règlement.

39 Voy. à cet égard, C. de Terwangne, « L'exception concernant les traitements de données à des fins personnelles et domestiques de la directive 95/46/CE relative à la protection des données : note d'observations sous Cour de justice de l'Union européenne (4e ch.), 11 décembre 2014 », *R.D.T.I.*, 2015, n° 58, pp. 39-51.

40 C.J.U.E., 11 décembre 2014, *František Ryneš c. Úřad pro ochranu osobních údajů*, aff. C-212/13.

41 Voy. C. de Terwangne, « Arrêt *Lindqvist* ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, n° 19, pp. 67-99.

42 C.J.C.E., 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy, Satamedia Oy*, aff. C73/07, n° 44.

données à caractère personnel sur internet sort de la sphère personnelle ou domestique par le fait que les données sont rendues accessibles à un nombre indéterminé et illimité de personnes[43]. Si la formulation du considérant pose question, il est prématuré d'en tirer des conclusions définitives sur sa portée exacte. Il convient en tout état de cause de souligner que ce n'est pas parce qu'une activité n'est ni professionnelle ni commerciale qu'elle tomberait dans le champ de l'exception.

B. Champ d'application territorial

12. Changement de paradigme et déjà de nouvelles zones d'ombre. Sur ce point des modifications substantielles sont à souligner par rapport aux critères d'application territoriale prévus dans la Directive. Il convient tout d'abord de rappeler le changement de paradigme. Sous le régime de la Directive, le critère de rattachement doit permettre de déterminer la ou les lois nationales applicables à un traitement de données. Dès lors que la réglementation sera désormais consolidée dans un règlement européen, il s'agira de déterminer si le Règlement s'applique ou non au traitement, sans référence à une loi nationale. Le « rattachement » d'un traitement de données à un territoire national devient théoriquement inutile, si ce n'est pour la question de la détermination de l'autorité de contrôle qui sera compétente pour connaître et sanctionner des irrégularités de traitement. Nous verrons que le Règlement fait sur ce point référence au lieu d'établissement du responsable du traitement ou du sous-traitant[44].

Reste une question de taille qui n'est pas – ou plutôt qui n'est plus – réglée par le Règlement : comme exposé ci-avant, les États membres conservent la possibilité de légiférer pour certains aspects ou types de traitements. Le Règlement ne définit pourtant pas quel sera le critère de rattachement dans ce cas[45]. Il s'agit donc d'une lacune juridique qui se profile et qui risque de créer une insécurité juridique, voire de mettre en péril l'objectif d'harmonisation si les États membres venaient à définir des critères d'application divergents. On peut toutefois imaginer que sur ces points, ce soient les règles de droit international privé qui soient exclusivement applicables pour déterminer la loi applicable. Cela n'était pas le cas jusqu'à présent en Belgique, par exemple, dès lors que la loi du 8 décembre 1992 était une loi transversale qui régissait les traitements de données indépendamment du secteur d'activité ou contexte dans lequel ils étaient mis en œuvre et qui contenait en son article 3*bis* son propre critère d'application territoriale.

13. La localisation de l'établissement du sous-traitant entrera en ligne de compte pour l'application territoriale du Règlement. Pour en revenir au Règlement, celui-ci reprend le premier critère d'application de la Directive, à savoir la localisation du lieu d'établissement. Le Règlement s'appliquera au traitement effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou – élément nouveau – d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union[46]. Les notions de « responsable du traitement » et de « sous-traitant » restent inchangées[47].

43 Cette assertion est émise par la Cour à la suite des gouvernements suédois et néerlandais et de la Commission européenne, points 47, 31, 32 et 33 de l'arrêt. Voy. également à ce sujet, l'avis du Contrôleur européen de la protection des données sur le paquet de mesures pour une réforme de la protection des données, 7 mars 2012, www.edps.europa.eu, p. 17.

44 Voy. *infra*, point 97.

45 Ce problème avait pourtant été soulevé par le Contrôleur européen de la protection des données dans son avis sur le paquet de mesures pour une réforme de la protection des données, 7 mars 2012, www.edps.europa.eu, p. 18.

46 Article 3, § 1er, du Règlement.

47 Articles 4, 7), et 4, 8), du Règlement.

Il conviendra donc de vérifier si le traitement a lieu *dans le cadre des activités* d'un établissement localisé sur le territoire de l'Union[48], peu importe la nationalité ou le lieu de résidence des personnes concernées par le traitement ou le lieu où les opérations de traitement sont réalisées. Concrètement, si une société établie aux États-Unis et qui traite des données de citoyens étasuniens fait appel à un sous-traitant établi sur le territoire de l'Union européenne, ce traitement sera soumis au Règlement.

Une question demeure ouverte : faudra-t-il dans ce cas considérer que le Règlement sera applicable à l'ensemble des opérations de traitement ou uniquement à celles de sous-traitance ? Si l'on s'en tient au texte du Règlement et aux considérants, on pourrait défendre l'idée qu'il ne s'agit que des opérations sous-traitées dès lors que le texte énonce que le Règlement s'applique au traitement de données à caractère personnel effectué dans le cadre *des activités d'un établissement d'un sous-traitant* sur le territoire de l'Union. Le lien avec les activités du sous-traitant pourrait donc conduire à restreindre l'application du Règlement aux seules opérations de traitement mises en œuvre par le sous-traitant. Reste que cela n'implique pas forcément que seul le sous-traitant serait soumis à des obligations en vertu du Règlement. Aucune restriction en ce sens n'est prévue dans le Règlement. Dès lors que le Règlement est applicable, il y a lieu de se référer, à notre sens, aux autres dispositions de celui-ci qui définissent les obligations et responsabilités respectives du responsable du traitement et du sous-traitant. Faire appel à un sous-traitant établi sur le territoire de l'Union peut donc avoir des conséquences importantes.

14. Le critère des moyens localisés sur le territoire d'un État membre passe à la trappe. Dans l'optique d'empêcher la délocalisation artificielle des responsables du traitement, il avait été prévu un critère auxiliaire dans la Directive : un responsable du traitement non établi sur le territoire d'un État membre mais qui fait usage de moyens, automatisés ou non, situés sur le territoire d'un État membre devait respecter la loi relative à la protection des données de cet État. Ce critère, appliqué par exemple à l'utilisation de cookies enregistrés sur des terminaux d'utilisateurs localisés sur le territoire d'un État membre[49], a soulevé des questions d'interprétation et de praticabilité. Il

[48] Cette notion a reçu sous le régime de la directive une interprétation large. Voy. à cet égard, l'analyse de la Cour du justice dans l'arrêt *Google Spain* qui précise que « l'article 4, § 1er, sous a), de la directive 95/46/CE exige non pas que le traitement de données à caractère personnel en question soit effectué "par" l'établissement concerné lui-même, mais uniquement qu'il le soit "dans le cadre des activités" de celui-ci » (C.J.U.E., 13 mai 2014, *Google Spain -Google Inc. c. Agencia Española de Protección de Datos (AEPD) – Mario Costeja González*, aff. C-131/12, no 52). Voy. également, l'arrêt *Weltimmo* qui précise qu'« il y a lieu de considérer que la notion d'"établissement", au sens de la directive 95/46/CE, s'étend à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable » (C.J.U.E., 1er octobre 2015, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, aff. C-230/14, no 31). Dans un arrêt du 28 juillet 2016, la Cour devait trancher la question de savoir si, lorsqu'une société basée au Luxembourg conclut des contrats de commerce électroniques avec des consommateurs situés sur un autre territoire, ce serait la loi de ce territoire qui trouverait à s'appliquer. Elle a considéré que l'article 4, § 1er, sous a), de la directive 95/46/CE doit être interprété en ce sens que pour qu'un traitement de données à caractère personnel effectué par une entreprise de commerce électronique soit régi par le droit de l'État membre vers lequel cette entreprise dirige ses activités, il faut que cette entreprise procède au traitement des données en question dans le cadre des activités d'un établissement situé dans cet État membre vers lequel l'activité est dirigée. Il appartient à la juridiction nationale d'apprécier si tel est le cas (C.J.U.E., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, aff. C-191/15).

[49] Voy. le document de travail du Groupe de l'article 29 du 30 mai 2002 sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur internet par des sites web établis en dehors de l'UE (p. 12).

implique par ailleurs une application extraterritoriale de la législation européenne avec la difficulté de contraindre des acteurs non établis sur son territoire à la respecter. Ce critère n'est plus repris dans le Règlement mais l'application extraterritoriale revient dans le Règlement par le biais de dispositions nouvelles.

15. De nouveaux critères liés à la localisation du public cible du traitement de données pour toucher les responsables du traitement établis hors de l'Union européenne. Sans doute inspirés par une volonté de réagir aux collectes et traitements à grande échelle de données de résidents européens par des sociétés établies en dehors de l'Union, deux nouveaux critères sont insérés à l'article 3 du Règlement pour rendre ce dernier applicable à des responsables du traitement non établis sur le territoire européen. Il est désormais prévu que le « règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

Ces deux critères ont en commun de déplacer la question de la localisation des moyens de traitement vers celle de la localisation du public cible du traitement des données.

Les considérants précisent, concernant le premier cas de figure que, pour établir l'intention d'offrir des biens ou des services à des personnes concernées qui se trouvent dans l'Union, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union, sont de possibles indicateurs clairs de cette intention[50]. Un parallèle peut être dressé avec le concept d'activité dirigée vers un ou plusieurs pays que l'on retrouve comme critère de rattachement en matière de droit de la consommation dans le Règlement sur la loi applicable aux obligations contractuelles[51] et le règlement sur la compétence judiciaire[52]. Il s'agira donc d'une analyse au cas par cas qui à la fois portera sur le fait qu'on rencontre le critère d'application du Règlement mais également qui consistera à déterminer quels sont les traitements « liés » à cette offre de biens ou de services qui seront soumis à celui-ci.

À première vue le second cas d'application extraterritoriale peut paraître bien large et quelque peu abscons. Il est question de « suivi du comportement qui a lieu au sein de l'Union ». Le considérant 24 du Règlement donne une interprétation plus restrictive de l'activité visée en précisant que « afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ulté-

50 En revanche, « la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention » (considérant 23 du Règlement).

51 *Cfr* article 6 du règlement (CE) n° 93/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I).

52 Article 17 du règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale.

rieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit». Il s'agit donc de suivi sur internet lorsqu'il y a profilage des personnes concernées grâce aux données collectées. On touche là, par exemple, typiquement à l'activité de publicité comportementale qui permet, sur la base du traitement d'informations sur le comportement d'un internaute sur le net (sites visités, produits consultés ou achetés) et d'une analyse dans la durée de ce comportement, de proposer des publicités ciblées. Rien n'exclut *a priori* que d'autres collectes massives de données par d'autres biais qu'internet (données de géolocalisation, données collectées par d'autres technologies telles que celles du *bluetooth* ou du RFID), puissent tomber dans le champ d'application de ce critère.

Un élément singulier de ces deux critères est que le législateur européen prenne notamment pour hypothèse d'application le cas où ces traitements liés à l'offre de biens ou de services ou de suivi comportemental sont le fait d'un sous-traitant. Nous ne voyons pas l'intérêt de prévoir cette hypothèse dans la mesure où le sous-traitant agit pour le compte et sur instruction d'un responsable du traitement. Autrement dit, si c'est l'activité qui est visée comme élément déclencheur de l'application du Règlement, elle est nécessairement le fait d'un responsable du traitement, la circonstance que des opérations techniques puissent être confiées à un sous-traitant n'ayant pas d'incidence dès lors que par définition le sous-traitant ne décide pas des finalités et moyens de traitement. On peut toutefois en retenir que le Règlement entend ne pas différencier l'hypothèse d'une activité réalisée par le responsable du traitement de celle confiée à un sous-traitant. Dans tous les cas de figure, le Règlement s'appliquera.

16. Le rôle du représentant renforcé. Comme auparavant, le Règlement entend assurer une certaine effectivité à cette application de la réglementation à des acteurs localisés hors de l'Union en créant une obligation de désigner un représentant établi sur le territoire de l'Union[53]. Élément nouveau, cette obligation s'applique au sous-traitant établi hors de l'Union mais qui est tenu d'appliquer le Règlement à des traitements[54]. Le représentant sera l'interlocuteur à qui devront s'adresser les autorités de contrôle et les personnes concernées et il devra répondre vis-à-vis d'elles du respect des obligations du responsable du traitement ou du sous-traitant qui l'aura désigné par écrit en cette qualité. Le considérant 80 du Règlement va même jusqu'à préciser que «le représentant désigné devrait faire l'objet de procédures coercitives en cas de non-respect du présent règlement par le responsable du traitement ou le sous-traitant». On peut craindre qu'il ne soit pas aisé de trouver preneur pour assumer ce rôle…

Le Règlement prévoit d'ailleurs des exceptions à cette obligation de désignation qui restreignent les hypothèses dans lesquelles une telle désignation sera requise. L'obligation ne s'appliquera pas lorsque le responsable du traitement est une autorité publique ou un organisme public ou encore lorsque le traitement est occasionnel, n'implique pas le traitement de données sensibles à grande échelle ni de données judiciaires et n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des

53 Pour une définition de cette notion, voy. article 4, 17), du Règlement.

54 Article 27 du Règlement.

finalités du traitement[55]. La seconde hypothèse appelle donc à nouveau une appréciation au cas par cas du caractère « risqué » ou non du traitement pour les droits et libertés concernés. En résumé, pour les traitements non « dangereux », il n'y aura pas d'interlocuteur sur le territoire européen qui doit être désigné.

IV. REDÉFINITION DE CERTAINS ASPECTS-CLÉS DU TRAITEMENT

A. Principes de licéité des traitements de données

17. Chapitre de « Principes ». Alors que la Directive, et avant elle déjà la Convention 108, rassemblait sous un seul chapitre les principes de base de la protection des données relatifs à la qualité des données et aux conditions de légitimation des traitements de données ordinaires et sensibles, mais aussi aux droits des personnes concernées et aux obligations des responsables du traitement, le Règlement met un peu d'ordre dans la présentation des choses. Désormais, les droits et obligations font l'objet de chapitres séparés. Quant aux conditions de licéité des traitements de données, elles sont présentées sous un chapitre sobrement intitulé « Principes ».

Comme auparavant, deux dispositions-clés de ce dernier chapitre énoncent, l'une (l'article 5), les principes relatifs au traitement des données à caractère personnel, et l'autre (l'article 6), les hypothèses dans lesquelles les traitements de données sont licites. Les articles 7 et 8 apportent des précisions nouvelles sur un élément qui a suscité de vifs débats lors du travail du législateur européen : le consentement de la personne concernée à ce que l'on traite ses données. Par ailleurs, les conditions de traitement des données sensibles sont également reprises dans ce chapitre de principes. Enfin, une hypothèse particulière fait son apparition, celle des traitements de données ne nécessitant pas l'identification des personnes concernées.

18. Principes de base de la protection des données. L'article 5 énonce l'ensemble des principes-clés réalisant la protection des données : principes de licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; exactitude ; limitation de la conservation ; intégrité et confidentialité ; et responsabilité. Certains de ces principes sont repris et développés dans d'autres parties du texte du Règlement. C'est le cas du principe de transparence qui prendra la forme d'obligations d'information des personnes concernées, ainsi que des règles de sécurité des données et de responsabilité des différents acteurs.

Les principes fondamentaux de la protection des données ne sont pas modifiés par rapport à ce qui régit cette matière depuis plusieurs décennies. Ces principes issus des Lignes directrices de 1980 de l'OCDE[56] et de la Convention 108 du Conseil de l'Europe ont fait leurs preuves et ont démontré leur capacité à résister à l'épreuve du temps et à être appliqués dans des contextes techniques, économiques et sociaux totalement mouvants. Certains affinements ou compléments ont toutefois été apportés, ainsi qu'on le verra dans les paragraphes qui suivent.

19. Principe de licéité, loyauté et transparence. Dans un souci de clarté, les auteurs du Règlement ont souhaité faire figurer explicitement le principe de transparence aux côtés de l'exigence de traitement licite et loyal alors

[55] Article 27, § 2, du Règlement.

[56] OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (2013), C(80)58/FINAL, telles qu'amendées le 11 juillet 2013 par C(2013)79, www.oecd.org.

que la doctrine le rattachait jusqu'alors à l'exigence de loyauté[57]. Ce principe de transparence est explicité dans un long considérant[58] qui commence par préciser que le traitement des données doit être transparent à l'égard des personnes concernées, de même que «la mesure dans laquelle ces données sont ou seront traitées», expression dont on ne perçoit pas vraiment la portée réelle. Le considérant évoque en outre la qualité de l'information à fournir aux personnes concernées et son contenu, éléments qui font l'objet des articles 12 à 14 du Règlement[59]. Certaines précisions se rattachent davantage à l'exigence de loyauté. C'est notamment le cas de l'indication que les personnes doivent être informées des risques liés au traitement de leurs données. On ne retrouve pas pareille exigence dans le devoir d'information des articles 13 et 14. On imagine difficilement par ailleurs, cette exigence mise en pratique…

20. Principe de limitation des finalités. Présenté depuis 35 ans comme la véritable pierre angulaire de la protection des données, le «principe de finalité», tel qu'il est couramment nommé, exige que les données soient collectées pour des finalités déterminées, explicites et légitimes, et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités. Les finalités du traitement des données doivent donc être fixées et claires dès le début. On peut effectuer sur ces données toutes les opérations qui seront considérées comme compatibles avec ces finalités d'origine.

Cette notion d'utilisation «compatible» a suscité de nombreux questionnements dans la pratique et les auteurs du Règlement ont eu le souci de la baliser davantage. Le texte présente ainsi, à son article 6, paragraphe 4, une série de critères permettant d'établir si le traitement des données pour une autre finalité est compatible ou non avec la finalité de la collecte de départ. Il s'agit de tenir compte du lien pouvant exister entre les deux finalités, du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement, de la nature des données, ordinaires ou sensibles, des conséquences du traitement ultérieur et des garanties existantes[60].

Une autre nouveauté du Règlement est la clarification du fait qu'il est permis dans certaines circonstances de traiter des données à une fin différente de celle pour laquelle les données ont été collectées même si cette nouvelle finalité n'est pas compatible avec la première. Le projet initial du texte ouvrait en fait largement cette possibilité, réduisant par là le principe de finalité à la portion congrue, tandis que le Conseil était allé plus loin encore, soulevant de vives critiques[61], en proposant d'autoriser les traitements ultérieurs réalisés par le même responsable à des fins incompatibles pourvu que les intérêts légitimes de ce responsable ou d'un tiers priment sur les intérêts des individus concernés[62]. Le principe de finalité aurait bel et bien été vidé de son sens. Le texte final du Règlement est revenu à la vocation protectrice du principe de finalité tout en l'assouplissant

57 Article 5, 1er, a), du Règlement.
58 Considérant 39 du Règlement.
59 Voy. *infra*, point 67.
60 Voy. également, considérant 50 du Règlement.
61 Voy. not., Groupe de l'article 29, Communiqué de presse du 17 mars 2015 sur le chapitre II du GDPR; voy. également, Opinion 03/2013 on purpose limitation, 2 avril 2013, WP 203, pp. 36-37. Onze États membres, parmi lesquels la Belgique, avaient exprimé des réserves sur ce point.
62 Cette proposition était destinée à faciliter les opérations de Big Data (C. Burton, L. De Boel, Ch. Kuner, A. Pateraki, S. Cadiot et S. G. Hoffman, «The Final European Union General Data Protection Regulation», *Privacy and Security Law Report*, 15 PVLR 153, 25 janvier 2016, p. 6).

dans les deux seules hypothèses suivantes : en cas de consentement de la personne concernée pour le traitement de ses données à de nouvelles fins incompatibles ou si le traitement ultérieur des données à des fins incompatibles est basé sur le droit de l'Union ou d'un État membre[63].

Enfin, on signalera que certaines réutilisations des données sont, comme dans le texte de la Directive mais de façon quelque peu réduite, considérées comme compatibles moyennant certaines conditions[64]. Il s'agit des traitements ultérieurs « à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques »[65].

21. Principe de minimisation des données. Les données à caractère personnel faisant l'objet d'un traitement doivent, comme auparavant, être adéquates et pertinentes au regard des finalités du traitement. Plutôt que de devoir être en outre « non excessives », elles doivent désormais être « limitées à ce qui est nécessaire ». Il est précisé au considérant 39 que cela implique notamment que la durée de conservation des données soit limitée « au strict minimum ». Le projet de texte émanant de la Commission ajoutait que le fait que les données soient limitées au minimum nécessaire exigeait de « veiller à ce que les données collectées ne soient pas excessives »[66]. Même si ce passage n'est pas repris dans le texte final du Règlement, il est à noter que le critère de nécessité s'exprime tant au niveau de la quantité des données que de leur qualité. Ainsi, s'il est clair qu'on ne peut traiter un nombre excessif de données (demander à un employé l'ensemble de son dossier médical pour juger de son aptitude au travail, notamment), on ne peut davantage se lancer dans le traitement d'une seule donnée qui porterait excessivement atteinte à la personne concernée (collecter l'information sur la sérologie VIH d'un candidat dans une procédure de recrutement pour un poste administratif, par exemple)[67]. Par ailleurs, le principe de minimisation des données conduit à ce que l'on ne puisse traiter des données à caractère personnel que lorsqu'il n'y a pas raisonnablement moyen d'atteindre la finalité sans cela[68].

22. Principe d'exactitude. Déjà présente dans les textes antérieurs, l'exigence que les données soient exactes et, si nécessaire, tenues à jour est reprise dans le Règlement. Toute inexactitude doit être corrigée, l'article 5, paragraphe 1er, d), apportant cette précision que la rectification doit être faite « sans tarder ».

23. Principe de limitation de la conservation. Le Règlement n'apporte pas de véritable changement à l'interdiction de conserver les données sous une forme permettant l'identification des personnes au-delà du temps nécessaire à l'accomplissement des finalités liées au traitement de ces données. Toutefois, le considérant 39 suggère que des délais soient fixés par le responsable du traitement pour l'effacement des données ou pour une vérification pério-

63 Article 6, § 4, du Règlement.

64 Ces conditions sont développées à l'article 89, § 1er, du Règlement.

65 Article 5, § 1er, b) *in fine*, du Règlement. Comp. article 6.1.b de la directive 95/46 qui admet comme compatible le « traitement ultérieur à des fins historiques, statistiques ou scientifiques ».

66 Considérant 30 de la proposition de règlement publiée le 25 janvier 2012 par la Commission européenne, COM(2012) 11 final.

67 Dans ce sens, voy. l'explication de la notion de données « excessives » dans le Projet de rapport explicatif de la Convention 108 du Conseil de l'Europe, version du 2 juin 2016, disponible à l'adresse : www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Projet%20de%20rapport%20explicatif_Fr.pdf : « Cette disposition vise aussi bien les aspects quantitatifs que qualitatifs des données à caractère personnel. Des données qui seraient adéquates et pertinentes mais entraîneraient une ingérence disproportionnée dans les droits et libertés fondamentaux en jeu doivent être considérées comme excessives et ne pas être traitées ».

68 Considérant 39 du Règlement.

dique, afin de garantir que la conservation des données ne dépasse pas ce qui est nécessaire.

24. Principe d'intégrité et de confidentialité. Sous l'intitulé d'« intégrité et confidentialité », c'est le devoir classique, mais ô combien crucial aujourd'hui, de sécurité des données qui figure désormais au rang des principes de base. Ce principe reprend *grosso modo* les termes qui étaient contenus à l'article 17 de la Directive. Une section entière du chapitre dédié aux responsable et sous-traitant développe ce devoir de sécurité en apportant la nouveauté de l'obligation de notifier à l'autorité de contrôle, voire aux personnes concernées, les violations de données[69].

25. Principe de responsabilité (*accountability*). La liste des principes de base de la protection des données se termine par l'affirmation que revient au responsable du traitement la responsabilité du respect de tous ces principes et, nouveauté, que le responsable doit être à même de démontrer que son traitement est en conformité avec ces principes[70]. Cette obligation de s'assurer et d'être en mesure de démontrer que le traitement de données est effectué conformément au Règlement est reprise et développée à l'article 24 du Règlement consacré à la responsabilité du responsable du traitement[71].

B. Hypothèses de licéité des traitements de données

26. Hypothèses plutôt que conditions. L'article 6, paragraphe 1er, du Règlement stipule que le traitement de données à caractère personnel n'est licite « que si, et dans la mesure où, au moins une des conditions suivantes est remplie ». Il ne s'agit pas à proprement parler de conditions à remplir mais plutôt d'hypothèses dans lesquelles les traitements sont admis. La traduction française de la proposition de texte publiée par la Commission européenne en début de processus législatif diffère d'ailleurs, alors même que les mots anglais n'ont pas changé. Ainsi, la version anglaise énonce que le traitement de donnée n'est licite que si « *at least one of the following applies* », ce qui a d'abord été traduit par « l'une au moins des situations suivantes s'applique », avant de devenir, dans la version finale « au moins une des conditions suivantes est remplie ».

Ces hypothèses dans lesquelles il est légitime de traiter des données à caractère personnel correspondent à celles déjà admises par la Directive mais quelques changements importants sont apparus.

27. Le consentement de la personne concernée. Le Parlement européen a clamé l'importance de la place du consentement dans l'édifice de protection des données : « Le consentement devrait demeurer l'élément-clé de l'approche de la protection des données de l'Union européenne, puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données »[72]. Toutefois, le législateur européen a fortement insisté durant le processus d'élaboration du Règlement sur la nécessité de veiller à ce qu'il ne soit plus abusé du recours

69 Section 2 du chapitre IV consacré aux devoirs des responsable et sous-traitant, articles 32-34. Voy. *infra,* points 55 et s.

70 Cette dimension d'« être en mesure de démontrer le respect des règles » n'apparaît pas clairement dans le terme « responsabilité » auquel on préfère donc parfois le terme anglais d'« *accountability* » qui comprend bien, lui, l'idée de rendre des comptes.

71 Voy. *infra,* points 40 et s.

72 Comité LIBE du Parlement européen, Rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012)0011, C7-0025/2012, 2012/0011(COD), rapporteur J. Ph. Albrecht, 21 novembre 2013, Exposé des motifs, pp. 218-219.

au consentement et à ce que, lorsqu'un traitement repose sur le consentement des personnes concernées, ce consentement soit de qualité et soit donné dans un contexte tel qu'on se trouve face à la véritable expression de l'autonomie du sujet. Au-delà de la définition donnée du consentement[73] qui est enrichie par rapport à la définition contenue dans la Directive, et de la mention du consentement comme fondement de licéité des traitements, deux articles[74] apportent encore des précisions sur le sujet et de longs considérants[75] viennent éclairer l'ensemble. Il y a là les traces des discussions nourries sur la question qui ont émaillé l'action législative du Parlement et du Conseil et le trilogue qui a pris place avec la Commission par la suite[76].

Un des aspects ayant suscité d'âpres discussions est la qualité que doit présenter le consentement pour être admis comme fondement d'un traitement. Sous l'empire de la Directive, il devait être « indubitable » pour le traitement de données ordinaires et « explicite » pour les données sensibles. Dans les discussions concernant le projet de règlement, tant la Commission que le Parlement ont été d'avis que désormais il fallait exiger que le consentement soit explicite pour qu'il serve de fondement valide pour le traitement de toutes les données, ordinaires comme sensibles, afin de lutter contre la récolte facile de consentements de mauvaise qualité sur internet. Le Conseil n'a pas suivi cette option et au final on est revenu à la notion de « *unambiguous* » déjà présente dans la Directive mais traduite cette fois, non plus par « indubitable », mais sans doute plus justement par « univoque »[77]. Pour le traitement de données sensibles, un consentement explicite sera encore requis.

On notera le paradoxe de la version française du texte du Règlement qui définit la notion de consentement à l'article consacré aux définitions, mais n'utilise pas expressément ce terme dans les hypothèses de licéité des traitements puisqu'il est dit à l'article 6, paragraphe 1er, a), que le traitement est licite lorsque « la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques » plutôt que lorsqu'elle a « donné son consentement », comme mentionné dans la Directive.

On reviendra ultérieurement dans cette contribution sur cette notion capitale de consentement, dans la partie consacrée au renforcement des droits de la personne concernée[78].

28. Le contrat. Dans sa liste des hypothèses de licéité des traitements de données, le Règlement reprend le cas où le traitement est nécessaire à l'exécution d'un contrat ou de mesures précontractuelles.

29. La sauvegarde d'un intérêt vital. Le Règlement reste aussi dans la ligne de la Directive en autorisant les traitements effectués pour sauvegarder des intérêts vitaux de la personne concernée. Il ajoute toutefois qu'il peut s'agir également des intérêts vitaux d'une autre personne physique. Le considérant 46 offre un exemple de situation où le traitement

73 Article 4, 11, du Règlement.
74 Articles 7 et 8 du Règlement.
75 Considérants 32, 33, 42, 43 et 44.
76 Les discussions ont été éclairées notamment par l'opinion émise par le Groupe de l'article 29 sur la notion de consentement (Groupe de l'article 29, avis 15/2011 du 13 juillet 2011 sur la notion de consentement, WP 187).
77 L'article 7, § 1er, qui est consacré aux conditions applicables au consentement apporte un élément qui compense d'une certaine manière l'abandon du qualificatif « explicite » au profit de « univoque ». Il s'agit de l'obligation qui est faite au responsable du traitement d'être en mesure de démontrer que la personne concernée a donné son consentement au traitement de ses données. La fourniture d'une telle preuve est essentiellement envisageable en présence d'un consentement explicite.
78 Voy. *infra*, points 71 et s.

de données est justifié par la sauvegarde d'intérêts vitaux: lorsque le traitement est nécessaire à des fins humanitaires, par exemple pour suivre la propagation d'épidémies ou dans le cas de catastrophes naturelles.

30. L'obligation légale ou la mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Ces hypothèses de licéité étaient déjà présentes dans la Directive et le Règlement précise expressément que les États membres sont autorisés à maintenir les dispositions nationales sectorielles ou spécifiques qu'ils auraient été amenés à adopter sur cette base avant l'entrée en vigueur du Règlement. Les États peuvent à l'avenir également introduire de telles dispositions sectorielles[79]. Les paragraphes 2 et 3 de l'article 6 apportent toutefois des précisions sur les conditions encadrant ces hypothèses de licéité des traitements. Ainsi, le fondement de ces traitements doit être défini par le droit de l'Union européenne ou par le droit d'un État membre qui doit répondre à un objectif d'intérêt public et être proportionné à l'objectif légitime poursuivi. Le considérant 41 précise que cette base juridique ou cette mesure législative doit répondre aux exigences mises en lumière par la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne. Elle doit en conséquence être claire et précise et son application doit être prévisible pour les justiciables. Les finalités des traitements en cause doivent être définies dans cette base juridique ou être liées à la mission d'intérêt public ou à l'exercice de l'autorité publique[80].

On notera qu'il ne s'agit pas d'admettre des situations où des données seraient traitées sur la base d'une norme étrangère à l'Union européenne[81].

On relèvera aussi une restriction apparue entre le texte de la Directive et celui du Règlement. La Directive admettait les traitements de données nécessaires à l'exécution d'une mission d'intérêt public dont est investi non seulement le responsable du traitement mais aussi un tiers auquel les données sont communiquées. Le Règlement n'a pas repris cette hypothèse du tiers chargé d'une mission publique. Il faudra donc que ce tiers soit lui-même un responsable du traitement pour avoir désormais accès ou recevoir des données nécessaires à l'exécution de sa mission.

31. Les intérêts légitimes du responsable du traitement ou d'un tiers. Le Règlement apporte quelques modifications à cette dernière hypothèse de licéité des traitements qui est celle de la balance des intérêts. Derrière ces modifications somme toute mineures se cachent d'intenses discussions qui se reflètent quelque peu dans la densité des considérants attachés à cette disposition.

Le traitement de données est donc admis s'il est nécessaire «aux fins des intérêts légitimes»[82] du responsable du traitement ou

79 «La possibilité laissée aux États d'adapter les règles applicables aux traitements imposés par une loi nationale est par contre plus problématique. Elle est significative de la volonté des États de conserver une part de leur souveraineté dès lors qu'il s'agit d'une relation entre l'État ou l'une de ses entités et le responsable du traitement/citoyen. Aussi compréhensible qu'elle soit, cette possibilité de continuer à réglementer un grand nombre de traitements sur une base spécifique et nationale ouvre une brèche importante dans l'acquis censé apporter par le règlement: l'unification des règles au niveau européen» (Th. Leonard et D. Chaumont, «GDPR.expert, Article 6. Licéité du traitement», 20 avril 2016, disponible à l'adresse: www.gdpr-expert.eu/difficultes-probables.html?id=6).

80 Article 6, § 3, alinéa 2, du Règlement.

81 Ch. Kuner, «The European Commission's Proposed Data Protection Regulation: a Copernican Revolution in European Data Protection Law», *Privacy and Security Law Report*, 11 PVLR 06, 2 juin 2012.

82 Le texte anglais du Règlement est resté le même que celui de la Directive sur ce point mais la traduction française a, elle, varié. On est passé de la formulation

d'un tiers, « à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant »[83].

Le Parlement européen, fort dérangé par le flou attaché à cette hypothèse et l'insécurité juridique qui en découle inévitablement, a tenté de procéder à l'avance à la mise en balance des intérêts contradictoires en présence afin de déboucher sur une liste des traitements d'office autorisés et une liste de ceux *a priori* illicites[84]. Cette idée de listes a cependant soulevé de nombreuses critiques tenant à des problèmes de délimitation des traitements à classer d'un côté ou de l'autre, et à l'inévitable situation où l'on n'a pu tout prévoir et où une liste fermée bloque donc ce qui n'y figure pas. Le Parlement s'est donc ravisé et est revenu à une formulation générique de la mise en balance des intérêts contradictoires en présence.

Le considérant 47 apporte une précision qui provient également des discussions ayant eu lieu au Parlement mais qui n'est pas sans susciter la perplexité. Il indique que lorsque l'on met en balance les intérêts légitimes d'un responsable du traitement ou d'un tiers avec les intérêts ou les libertés et droits fondamentaux de la personne concernée, il faut tenir compte des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. Le texte spécifie : « En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée. Les intérêts et droits fondamentaux de la personne concernée pourraient, en particulier, prévaloir sur l'intérêt du responsable du traitement lorsque des données à caractère personnel sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur ». Faire intervenir le critère de l'attente raisonnable des personnes concernées est plutôt pertinent pour évaluer si une opération effectuée sur les données est bien compatible avec la finalité initiale. Et le fait que le considérant évoque *in fine* l'hypothèse d'un traitement ultérieur appuie cette impression que les auteurs du considérant confondent la balance des intérêts avec l'évaluation de la compatibilité des utilisations ultérieures des données au regard de la finalité initiale. Cette balance ne revient pas à mettre en jeu le fait que la personne concernée s'attend ou non au traitement effectué sur ses données. Des traitements de données peuvent s'avérer légitimes sur la base de la balance d'intérêts sans que la personne concernée ne s'attende nécessairement à ce que ses données fassent l'objet d'un traitement. C'est le cas, par exemple, d'un traitement de données effectué par un journaliste dans le cadre d'une enquête qu'il mène à l'égard d'un acteur politique. Ce dernier ne s'attend vraisemblablement pas à ce que des données soient rassemblées sur lui et pourtant l'intérêt de la liberté de la presse justifiera pleinement le traitement de données. De même, la collecte de données auprès de tiers à des fins de marketing direct échappe le plus souvent aux personnes concernées alors

« nécessaire à la réalisation des intérêts légitimes (…) » à une formulation moins heureuse « nécessaire aux fins des intérêts légitimes (…) ».

83 Article 6, § 1er, f), du Règlement.

84 Article 6, § 1er, b) et c), de la proposition de texte du Comité LIBE du Parlement européen (Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, COM(2012)0011, C7-0025/2012, 2012/0011(COD)), rapporteur J. Ph. Albrecht, 17 décembre 2012).

que de tels traitements sont reconnus comme légitimes. C'est le devoir d'information qui pèse sur le responsable[85] qui viendra éclairer les personnes concernées sur le sort réservé à leurs données.

Le Règlement offre des exemples de cas où le traitement peut légitimement se fonder sur une hypothèse de balance d'intérêts. Ainsi, il cite les traitements à des fins de prévention de la fraude ou à des fins de prospection commerciale[86] ou ceux visant à garantir la sécurité du réseau et des informations[87].

L'attention apportée à la fin de la disposition aux enfants (« notamment lorsque la personne concernée est un enfant ») ne doit être là sans doute que pour inviter à tenir compte, lors de la mise en balance, de l'éventuelle qualité d'enfant de la personne concernée, car cette portion de phrase n'induit rien de véritablement concret. Aucun écho de cette attention particulière ne se retrouve par ailleurs dans les considérants.

Enfin, on signalera que les auteurs du Règlement excluent expressément de cette hypothèse de licéité les traitements effectués par les autorités publiques dans l'exécution de leurs missions[88]. Pour ces traitements, l'exigence de légalité impose au législateur de prévoir par la loi la base juridique justifiant le traitement des données à caractère personnel par les autorités publiques[89].

C. Le traitement de données sensibles

32. Données sensibles par nature et selon le contexte. Le Règlement identifie, comme la Convention 108 et la Directive avant lui, des données telles celles relatives à l'origine raciale ou ethnique, aux opinions politiques ou à la santé qui sont, par nature, particulièrement sensibles du fait qu'elles mettent en jeu des libertés et droits fondamentaux. Le contexte dans lequel elles sont traitées peut engendrer des risques pour ces droits et libertés[90]. L'impact du contexte sur la nature sensible d'une donnée est surtout important en présence de données qui ne seront pas dans tous les cas à considérer comme sensibles. C'est le cas, par exemple, de la photo d'un individu. Elle révèle son origine raciale ou ethnique mais ce ne sera très souvent pas cet aspect-là qui sera traité lors de l'enregistrement et de l'utilisation de la photographie. Ce ne sera donc que dans le cas où le traitement de photos est réalisé afin d'établir l'origine raciale ou ethnique des individus apparaissant sur les clichés que les photos devront être considérées comme des données sensibles et seront protégées par le régime plus strict accordé à de telles données. Le considérant 51 apporte un autre exemple de l'impact du contexte de traitement sur la notion de données sensibles. Il s'agit encore du traitement de photographies mais cette fois pour en extraire des données biométriques. D'après le considérant, il ne faut pas faire systématiquement entrer toute photographie dans la définition de données biométriques. Ce ne sera que « lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique », comme dans le cas de badges utilisés pour accéder à des locaux, que les photos correspondront à des données biométriques et bénéficieront du régime restrictif des données sensibles.

33. Liste des données sensibles. Le Règlement a repris en l'étoffant quelque peu la liste des données sensibles figurant dans la Directive. Ainsi, à côté des données qui révèlent

85 Voy. *infra*, points 67 et s.
86 Considérant 47.
87 Considérant 49.
88 Article 6, § 1er, alinéa 2, du Règlement.
89 Considérant 47.
90 Considérant 51.

l'origine raciale et ethnique les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale et les données concernant la santé, la vie et l'orientation sexuelles, le Règlement ajoute désormais à la liste les données génétiques et les données biométriques traitées aux fins d'identifier une personne physique de manière unique[91].

34. Régime des données sensibles. Le même régime qu'avant est réservé à ces données, un régime plus protecteur que pour les données ordinaires étant donné le risque plus élevé que leur traitement engendre pour la personne concernée. Pour ces données, c'est le principe d'interdiction de traitement qui prévaut, assorti d'exceptions pour lesquelles leur traitement est admis[92].

Comme auparavant, une marge de manœuvre est laissée aux États membres qui peuvent prévoir d'autres dérogations que celles énoncées par le Règlement, mais seulement pour des motifs d'intérêt public important. À la différence de la Directive, le Règlement précise que ces dérogations doivent être prévues par le droit national « qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »[93].

35. Les données relatives aux condamnations pénales et aux infractions. Une disposition spécifique[94] est consacrée au traitement des données relatives aux condamnations pénales et aux infractions ou mesures de sûreté connexes[95]. Ce qui est prévu est sommaire et très semblable à ce qui figurait dans la Directive[96]. On rappellera que les traitements de données effectués par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes, de poursuites et d'exécution de sanctions pénales sont désormais couverts par la directive 2016/680 du 27 avril 2016[97].

36. Les numéros d'identification uniques. Comme la Directive, le Règlement s'en remet aux États membres pour décider d'autoriser l'utilisation d'un numéro d'identification unique ou de tout autre identifiant de portée générale[98]. Le texte impose toutefois, et c'est nouveau, aux États qui optent pour le recours à un tel identifiant de prévoir des garanties appropriées pour les droits et libertés de la personne concernée.

D. Dispense d'identification des personnes concernées

37. Pas de nécessité de collecte d'informations supplémentaires. Une disposition nouvelle particulièrement pertinente et bienvenue a été insérée dans le Règlement. Il s'agit de l'article 11 selon lequel si les données traitées par un responsable du traitement ne permettent pas à celui-ci d'identifier une personne physique, il n'est pas obligé d'obtenir des informations supplémentaires pour identifier la personne en question à la seule fin de respecter le Règlement. Cette disposition vise, par exemple, le cas où une caméra a été placée

91 Article 9 du Règlement.
92 Voy. les dix exceptions prévues à l'article 9, § 2, a) à j), du Règlement.
93 Article 9, § 2, g), du Règlement.
94 Article 10 du Règlement.
95 Ces données sont mentionnées dans la suite du présent texte sous l'appellation de « données judiciaires ».
96 Article 8, § 5, de la Directive.
97 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, n° L 119/89, 4 mai 2016.
98 Article 87 du Règlement.

sur un immeuble filmant les allées et venues à l'entrée. Les images filmées sont des données à caractère personnel dès lors que les personnes sont identifiables, même si le propriétaire de l'immeuble ne procède pas lui-même à l'identification des personnes entrant et sortant. L'article 11 du Règlement dispense le responsable de ce traitement de chercher à identifier les individus filmés juste pour être à même de leur répondre s'ils souhaitent exercer leurs droits d'accès, de rectification ou d'opposition. Dans le même sens, le chercheur qui travaille avec des données codées obtenues à diverses sources ne devra pas se fournir la clé des codes ni les informations de contact pour honorer son obligation d'information des personnes concernées.

L'idée est donc que les règles de protection des données n'aboutissent pas à la situation paradoxale où l'on doive en connaître davantage sur les personnes à propos de qui on traite des données pour garantir la protection de leurs données.

V. RESPONSABILISATION ACCRUE DES ACTEURS

A. Sous l'angle de la prévention des risques

38. Plus de responsabilités pour une protection des données plus effective. Un trait saillant du Règlement est l'accent mis sur une responsabilisation accrue des acteurs du traitement que sont le responsable du traitement et le sous-traitant.

Il se marque tout d'abord sous l'angle de la prévention des risques que peut engendrer pour les libertés et droits individuels le traitement de données. Le Règlement impose de nouvelles obligations ou entérine des pratiques existantes qui tendent à contraindre le responsable du traitement à pouvoir démontrer non seulement qu'il a vérifié que son traitement était conforme aux exigences légales, mais qu'il a par ailleurs analysé les risques, qu'il a pris les mesures adéquates pour protéger les données en fonction du niveau de risques et que ces mesures ont été respectées.

39. Le rôle du sous-traitant, entre exécutant et conseiller avisé. Par ailleurs, de nouvelles obligations sont directement mises à charge du sous-traitant[99]. Si le principe reste celui d'une obligation de conclure un contrat entre le sous-traitant et le responsable du traitement, le Règlement précise davantage ce qui doit être contractuellement organisé et prévoit des obligations plus étendues dans le chef du sous-traitant[100]. Parmi celles-ci figurent l'obligation d'aider le responsable du traitement dans la suite à donner à l'exercice des droits des personnes concernées, une obligation d'assistance dans l'analyse d'impact dont il sera question ci-après et une obligation de supprimer ou de restituer, au choix du responsable du traitement, les données traitées à la fin de la mission de sous-traitance.

En outre, le Règlement va encore plus loin dans la responsabilisation du sous-traitant. Tout comme sous le régime de la Directive, ce dernier ne peut agir que sur instruction du responsable du traitement, instruction qui devra toutefois être documentée lorsque le Règlement entrera en application. Cependant, le Règlement ne cantonne pas le sous-traitant à un rôle de simple exécutant et requiert qu'il informe immédiatement le responsable du traitement s'il estime qu'une instruction qui lui est donnée constitue une violation du Règlement ou d'autres dispositions du droit de l'Union ou du droit national relatives à la protection des données[101].

99 Article 28 du Règlement.
100 Article 28, § 3, du Règlement.
101 Article 28, § 3, h), alinéa 2, du Règlement.

1. Le principe de responsabilité (accountability)

40. Respecter la réglementation n'est plus suffisant : il va falloir pouvoir le démontrer. Ce principe est inscrit à l'article 5, paragraphe 2, du Règlement. Il vient sanctionner les autres principes-clés du traitement que nous avons évoqués ci-dessus[102].

Le responsable du traitement, comme sous le régime de la Directive, est tenu de respecter les principes du traitement mais il est désormais spécifié qu'il doit démontrer que ceux-ci sont respectés[103]. C'est ce que désigne ce « principe de responsabilité » entendu non pas comme impliquant essentiellement une obligation de réparer le dommage en cas de violation de la réglementation[104], mais qui s'apparente davantage à l'idée de « répondre de », en l'occurrence répondre des mesures prises pour s'assurer du respect de la réglementation (le concept étant mieux traduit par le terme anglais d'« *accountability* », distinct de celui de « *liabiltiy* » qui subsiste par ailleurs[105]). Cela suppose donc une certaine proactivité et anticipation des critiques que l'on pourrait formuler à l'égard d'un traitement.

41. Incidence au niveau de la charge de la preuve. On peut par ailleurs se demander si l'introduction du principe d'*accountability* dans la réglementation engendrera un allègement de la charge de la preuve en matière de responsabilité (*liability*) au profit de la personne concernée une fois le Règlement applicable. Jusqu'alors, il appartenait à l'individu victime d'un préjudice causé par une violation des règles applicables en matière de protection des données de démontrer l'acte contraire à la réglementation du responsable du traitement, le dommage causé et le lien causal entre cet acte contraire et ce dommage[106]. Lorsque le Règlement sera d'application, le responsable du traitement devra, en vertu de l'article 5, paragraphe 2, du Règlement, être en mesure de démontrer qu'il respecte la réglementation. On peut dès lors se demander si à l'avenir l'individu ayant introduit un recours judiciaire devra démontrer une violation du Règlement ou simplement alléguer qu'une telle violation existe, reportant ainsi le fardeau de la charge de la preuve dans le chef du responsable du traitement. Ce qui est toutefois certain c'est qu'une fois la non-conformité au Règlement établie, il appartient au responsable du traitement ou au sous-traitant d'établir que le dommage causé ne lui est pas imputable pour s'exonérer de sa responsabilité[107].

42. Les situations respectives du responsable du traitement et du sous-traitant en termes d'*accountability*. Ce principe général d'*accountability* applicable à tout traitement prend corps avec des obligations particulières pour certains types de traitements ou responsables de traitement, qui formalisent les mesures à prendre par le responsable du traitement pour s'assurer du respect des principes de protection. Nous les détaillerons ci-dessous. Nous verrons que certaines de ces obligations sont également imposées au sous-traitant, sans pourtant que ce dernier ne soit formellement tenu de respecter le principe d'*accountability* vis-à-vis des autorités de contrôle ou des personnes concernées. En revanche, il lui est fait obligation de mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer qu'il

102 Voy. *supra*, point 25.
103 Article 5, § 2, du Règlement.
104 Comp. article 23 de la Directive intitulé « responsabilité ».
105 Voy. *infra*, points 61 et s.
106 Article 15*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.
107 Article 82, § 3, du Règlement.

respecte les obligations qui lui incombent en vertu de l'article 28 du Règlement[108].

2. *Le registre des traitements*

43. Un registre des activités de traitement et plus de déclaration préalable. L'obligation de notification préalable des traitements à l'autorité de contrôle disparaît au profit d'autres obligations. L'article 30 du Règlement prévoit une obligation générale pour les responsables du traitement de tenir un registre des activités de traitement et pour les sous-traitants de tenir un registre des catégories d'activités de traitement. Il s'agit d'identifier dans un document écrit différentes caractéristiques des traitements énoncées dans le Règlement (finalités, catégories de données traitées, catégories de personnes concernées, etc.) et de tenir ce document à disposition de l'autorité de contrôle.

44. Portée limitée des exemptions. Sont exemptées de cette obligation les organisations ou entreprises, qu'elles soient responsables du traitement ou sous-traitants, qui comptent moins de 250 employés. Si *a priori* cette exemption semble bien large, il n'en est rien. Elle ne vaut plus si le traitement mis en œuvre est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur des données sensibles. Il s'agit là encore d'une appréciation au cas par cas mais on peut d'ores et déjà anticiper qu'il sera rare qu'une entreprise ne traite des données à caractère personnel qu'*occasionnellement*. Les exemptions à l'obligation de notification préalable dans la loi belge ne prenaient d'ailleurs pas exactement les mêmes critères en compte. L'arrêté royal du 13 février 2001[109] prévoyait des exemptions de la formalité de notification pour des finalités types de traitements assez « banals » en entreprise (administration du personnel et des salaires, gestion de la clientèle et des fournisseurs, etc.), par exemple. Il en résulte que si la suppression d'une notification préalable est la bienvenue dès lors que cette formalité assez fastidieuse n'a pas prouvé son efficacité pour garantir un bon niveau de respect de la protection des données, les obligations en termes de documentation – cette fois interne – relatives aux traitements opérés par le responsable et le sous-traitant seront sans doute plus systématiques sous le régime du Règlement.

3. *L'analyse d'impact*

45. Identification des risques. En sus de l'obligation de documentation que l'on vient d'évoquer, le Règlement prévoit dans certains cas une obligation de réaliser une analyse de risques. L'enjeu est de déterminer quelles mesures prendre pour prévenir le ou les risques identifiés. La première étape sera de déterminer dans quelles hypothèses une telle analyse est requise. L'article 35, paragraphe 1er, du Règlement prévoit que l'analyse s'impose lorsque « un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[110].

[108] Article 28, § 3, h), du Règlement.

[109] Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001.

[110] Voy. pour les exceptions à l'obligation d'effectuer une analyse d'impact l'article 35, § 10, du Règlement. Elles concernent les traitements (1) mis en œuvre par un responsable devant se conformer à une obligation légale définie par le droit national, (2) qui interviennent dans le cadre d'une mission d'intérêt public ou (3) qui relèvent de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Omniprésente dans le Règlement, cette notion de «risque» n'est pas définie[111]. Dans une version intermédiaire de la proposition de règlement[112], on citait comme exemples de risques potentiels, une discrimination, un vol ou une usurpation d'identité, une perte financière, une atteinte à la réputation, un renversement non autorisé de la pseudonymisation, une perte de confidentialité de données protégées par le secret professionnel ou plus généralement «tout autre dommage économique ou social important»[113].

Il s'agira d'apprécier le risque au cas par cas – et le Groupe de l'article 29 annonce la publication d'un document consacré à cette question[114] –, mais le Règlement identifie d'ores et déjà quelques balises. Il mentionne trois hypothèses dans lesquelles l'analyse est requise: (i) la surveillance systématique à grande échelle d'une zone accessible au public (par exemple, grâce à l'utilisation des dispositifs de surveillances opto-électroniques[115]), (ii) le traitement à grande échelle de données sensibles[116], ainsi que (iii) en cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire. Ce dernier cas de figure vise, par exemple, le traitement de *big data*.

46. Remédiation aux risques. L'analyse de risques doit déboucher sur la définition et l'adoption de mesures pour faire y face.

L'exercice n'implique pas seulement une démarche de réflexion. Il doit également être documenté et conduire à la réalisation d'un document écrit dont le contenu minimum est arrêté dans le Règlement[117]. L'analyse d'impact requerra, à notre sens, des compétences pluridisciplinaires puisqu'il y est à la fois question d'atteintes à des droits (par exemple, le droit de ne pas subir de discrimination), de conséquences sociales dommageables ou encore de failles techniques qui pourraient mettre en péril l'intégrité ou la confidentialité de données. Il se pourrait donc qu'on doive, hormis pour de grandes entreprises déjà rompues à ce genre d'exercice, se tourner vers des entreprises spécialisées pour réaliser ces analyses d'impact.

47. Consultation de l'autorité de contrôle. Ces obligations se doublent d'une obligation pour le responsable du traitement de

111 C. Burton, L. De Boel, Ch. Kuner, A. Pateraki, S. Cadiot et S. G. Hoffman estiment que pour déterminer les traitements de données présentant «*a risk*» ou «*a high risk*», «*guidance is needed on this topic to help companies assess with a reasonable level of certainty the level of risk related to their data processing activities*» (C. Burton, L. De Boel, Ch. Kuner, A. Pateraki, S. Cadiot et S. G. Hoffman, «The Final European Union General Data Protection Regulation», *Privacy and Security Law Report*, 15 PVLR 153, 25 janvier 2016, p. 7).

112 Version consolidée du 11 juin 2015 de la Proposition de règlement après la réunion du Coreper du 9 juin 2015, http://data.consilium.europa.eu/doc/document/ST-9788-2015-INIT/en/pdf.

113 Voy. pour un outil d'analyse article par article du règlement et de ses différentes versions: www.gdpr-expert.eu.

114 Groupe de l'article 29, «Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)», WP 236, 2 février 2016.

115 Considérant 91 du règlement.

116 Le considérant 91 du règlement précise que ne devrait pas être considéré comme étant à grande échelle, le traitement qui concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat *exerçant à titre individuel*.

117 Article 35, § 7, du Règlement. Il n'y a que peu d'indications dans le règlement sur ce qui est attendu de la part du responsable du traitement. Pour un exemple de méthodologie, voy. les documents de la CNIL (Commission nationale de l'informatique et des libertés) relatifs aux analyses d'impact accessibles à l'adresse: www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil.

consulter l'autorité de contrôle préalablement au traitement lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque *élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque*[118]. Les considérants 84 et 94 du Règlement jettent un doute sur la manière d'interpréter les circonstances qui doivent déclencher cette obligation de consultation préalable puisqu'il y est expliqué que la consultation préalable s'impose lorsqu'il s'avère que le responsable du traitement *ne peut atténuer le risque élevé* identifié par l'adoption de mesures.

En tout état de cause, cette obligation devrait permettre à ladite autorité d'être informée de l'intention de mettre en œuvre un traitement potentiellement problématique et de pouvoir, dans un délai de réaction de huit semaines, prolongeable dans certains cas, émettre un avis sur le traitement et mettre en œuvre ses prérogatives de contrôle qui se sont considérablement étendues comme on le verra. Il s'agit donc là d'un retour d'une forme de notification préalable mais limitée aux traitements qui présentent les risques les plus élevés[119].

L'autorité de contrôle peut ainsi conseiller le responsable du traitement sur ce qu'il convient de faire[120] ou, entre autres mesures possibles, lui interdire la mise en œuvre de traitement. Rien n'est prévu si l'autorité de contrôle ne réagit pas dans le délai imparti. Il ne s'agira toutefois pas de considérer cette absence de réaction comme une autorisation tacite de mettre en œuvre le traitement. Le considérant 94 du Règlement indique en effet que « l'absence de réaction de l'autorité de contrôle dans le délai imparti devrait être sans préjudice de toute intervention de sa part effectuée dans le cadre de ses missions et de ses pouvoirs prévus par le présent règlement, y compris le pouvoir d'interdire des opérations de traitement ».

4. Le délégué à la protection des données

48. Une nouvelle fonction pour qui et pour quoi ? De spécialiste, il en sera également question avec l'introduction dans le Règlement d'un nouvel acteur, le délégué à la protection des données (*data protection officer*), désigné par le responsable du traitement ou par un sous-traitant[121]. C'est d'ailleurs l'un des seuls éléments requis concernant le délégué à la protection des données : qu'il dispose de connaissances spécialisées du droit et des pratiques en matière de protection des données pour pouvoir informer et conseiller le responsable du traitement ou le sous-traitant qui l'aura désigné et servir de point de contact avec l'autorité de contrôle ou des personnes concernées[122]. Le délégué peut être un membre du personnel ou un tiers prestant dans le cadre d'un contrat de services[123]. Le Règlement se focalise sur des critères de compétence et des garanties pour que le délégué puisse avoir une connaissance effective des activités de traitement et travailler de manière indépendante et sans crainte de se voir sanctionner pour les avis ou conseils qu'il donne[124]. Le Règlement

118 Article 36 du Règlement.

119 À noter que les États membres pouvaient déjà, en vertu de l'article 20 de la Directive, définir des types de traitements qui devaient faire l'objet d'un examen préalable par l'autorité de contrôle.

120 Article 58, § 3, a), du Règlement.

121 Article 37 du Règlement. La notion n'est toutefois pas tout à fait neuve dès lors qu'elle existait déjà notamment dans le règlement 45/2001 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 (voy. le chapitre 8 dudit Règlement) et que plusieurs États membres avaient instauré une fonction semblable dans leur législation.

122 Article 37, § 5, du Règlement. Pour les fonctions du délégué, voy. article 39, § 1er, du Règlement.

123 Article 37, § 6, du Règlement.

124 Article 38, §§ 2 et 3, du Règlement.

précise notamment que le délégué ne peut être pénalisé ou relevé de ses fonctions pour l'exercice de ses fonctions.

49. Le caractère obligatoire ou optionnel de la désignation. Concrètement, tout responsable du traitement ou sous-traitant peut s'adjoindre les services d'un délégué à la protection des données, ce qui entraînera alors l'application du Règlement audit délégué, notamment en ce qui concerne les protections contre un licenciement ou une rupture de contrat[125]. Dans certains cas, il devra le faire. Il s'agit tout d'abord des traitements effectués par une autorité publique ou un organisme public, exception faite toutefois des juridictions agissant dans l'exercice de leur fonction juridictionnelle[126]. Pour le secteur privé, la désignation d'un délégué à la protection des données sera requise lorsque les activités de base du responsable du traitement ou du sous-traitant (et donc pas lorsque les traitements ne sont effectués qu'en tant qu'activité auxiliaire) consistent (i) en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ou encore (ii) en un traitement à grande échelle de données sensibles ou judiciaires[127]. Le Règlement laisse toutefois la possibilité aux États membres ou au droit de l'Union d'imposer la désignation d'un délégué dans d'autres hypothèses[128].

50. Une nouvelle collaboration qui reste à définir. Le Règlement demeure somme toute assez succinct sur le sujet et n'aborde pas, par exemple, les modalités de désignation du délégué ou les questions de responsabilité du délégué vis-à-vis de l'entité qui l'a désigné, les modalités de collaboration demeurant pour le reste largement à définir. Ainsi on pourra se demander comment combiner des possibilités de sanctionner une faute du délégué dans l'exercice de ses missions avec la protection dont il bénéficie contre sa mise à pied. Le Groupe de l'article 29 a toutefois annoncé qu'il publierait des lignes directrices sur le sujet en vue de l'entrée en vigueur du Règlement[129].

5. Protection dès la conception et par défaut

51. Pour une protection paramètre d'usine. Face à la complexité et à l'opacité des traitements de données dans un contexte où de nombreuses activités sont désormais effectuées par le biais du numérique, il paraît logique que les équipements ou applications qui traitent les données soient, à l'origine, conçus et paramétrés pour tenir compte des enjeux en matière de vie privée.

L'idée est séduisante mais la difficulté est de toucher les fournisseurs ou fabricants qui eux-mêmes ne traitent pas les données. Le Règlement fera peser, de fait, les obligations dès la conception (*protection by design*) et la protection par défaut (*protection by default*) sur le responsable du traitement en lui imposant de faire le choix de moyens, y compris technolo-

125 Article 37, §§ 1er et 4, du Règlement. Se posera donc la question de la qualification de la fonction qui sera dévolue à un juriste chargé des aspects de protection de données au sein d'une entreprise qui n'est pas tenue de désigner un délégué à la protection des données dès lors que la qualité de délégué à la protection des données entraîne une série de garanties et d'obligations vis-à-vis de ce dernier qui sont prévues dans le Règlement.

126 Article 37, § 1er, a).

127 Article 37, § 1er, a) et b), et considérant 97 du Règlement.

128 Article 37, § 4, du Règlement.

129 Groupe de l'article 29, « Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR) », WP 236, 2 février 2016. Au moment d'écrire ces lignes, le Groupe de l'article 29 n'avait pas encore publié ses « Guidelines on Data Protection Officers ('DPOs') », WP 243, adoptées le 13 décembre 2016, disponibles désormais à l'adresse http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

giques, qui permettent de respecter les principes en matière de protection des données.

52. Lorsque l'activité doit s'adapter à la protection des données. La protection dès la conception impose au responsable du traitement de façonner son traitement de manière à assurer la protection la plus effective possible des droits des personnes concernées. Ainsi doit-il adopter, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du Règlement et de protéger les droits de la personne concernée[130]. Il s'agit donc de taper sur le clou en rappelant qu'il faudra être proactif et pouvoir démontrer qu'on a pris des mesures qui permettent d'assurer effectivement les principes du Règlement énoncés à l'article 5 du Règlement. Ces mesures tiendront compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques que présente le traitement pour les droits et libertés des personnes physiques. On cite l'exemple de la minimisation des données traitées (ce qui conduirait à bannir les systèmes – nombreux sur le marché – qui recueillent des données non justifiées) et le recours à la pseudonymisation[131] des données dès que cela s'avère possible au regard des finalités poursuivies[132].

53. Lorsque la technique doit s'adapter à la protection des données. La protection par défaut met l'accent sur l'adoption de mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Le Règlement précise que « cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée »[133].

La responsabilité de choisir des produits *privacy friendly* incombe dès lors au responsable du traitement mais avec l'objectif non dissimulé du législateur européen d'influer sur les fabricants de produits, les prestataires de services et les producteurs d'applications. Il est évident que ces prestataires et producteurs seront impactés par le Règlement et sensibilisés à davantage prendre en compte la dimension de protection des données dans la conception de leurs produits et services dès lors qu'ils s'adresseront à une clientèle tenue de respecter le principe de protection par défaut[134].

B. Sous l'angle de la gestion des risques

54. Le Règlement introduit non seulement un certain nombre de nouvelles dispositions relatives à la prévention des risques que nous venons d'examiner, mais il va plus loin en prévoyant des mesures permettant de gérer les risques encourus en matière de protection des données à caractère personnel.

1. Notification des violations de données à caractère personnel

55. Faille dans la sécurité des données. Afin de garantir la sécurité des données,

130 Article 25, § 1er, du Règlement.
131 Il s'agit d'un nouveau concept défini à l'article 4, 5), du Règlement, qui vise le codage des données, plutôt que leur anonymisation pure et simple.
132 Considérant 78 du Règlement.
133 Article 25, § 2, du Règlement.
134 Voy. considérant 78 du Règlement.

celles-ci doivent être traitées de façon à ce que leur sécurité soit garantie de manière appropriée, à l'aide des mesures techniques ou organisationnelles adéquates[135]. Les données doivent notamment être protégées contre les traitements non autorisés ou illicites et contre la perte, la destruction ou les dégâts d'origine accidentelle en vue de préserver leur intégrité et leur confidentialité. Toutefois, aucun responsable de traitement n'est à l'abri d'une faille de sécurité, les *hackers* faisant sans cesse preuve d'inventivité pour pénétrer les systèmes informatiques. De telles failles de sécurité peuvent entraîner la perte, l'altération ou la divulgation de données personnelles et être préjudiciables tant pour l'individu que pour le responsable du traitement.

56. Obligation de notification. Sous la Directive, aucune obligation générale de notifier les violations de données à l'autorité nationale compétente n'est prévue. En Belgique, seules les entreprises actives dans le secteur des télécoms et tombant sous le coup de la loi du 13 juin 2005 relative aux communications électroniques et du règlement européen n° 611/2013 du 24 juin 2013[136] concernant les mesures relatives à la notification des violations de données à caractère personnel devaient jusqu'ici notifier les violations de données à la Commission de la protection de la vie privée et, dans certaines hypothèses, aux personnes concernées également. Pour les autres secteurs d'activités, la Commission de la protection de la vie privée a émis une recommandation d'initiative[137] à l'attention des responsables du traitement leur demandant, sur base volontaire, de lui notifier endéans les 48 heures les cas d'incidents et d'informer le public dans les deux jours suivant cette notification.

Une fois le Règlement applicable, tous les responsables du traitement auront une obligation légale de notifier les violations de données à caractère personnel dont ils sont victimes. On pourrait penser que l'obligation de notification se limite à la fuite accidentelle de données. Tel n'est pas le cas. Le Règlement définit la violation de données comme étant « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »[138]. Compte tenu de cette définition extensive, les notifications auprès de l'autorité de contrôle interviendront plus souvent qu'on aurait pu le penser.

Les dispositions du Règlement constituent donc une nouveauté en la matière en ce qu'elles prévoient que les violations de données à caractère personnel que subit le responsable du traitement doivent être notifiées à l'autorité de contrôle endéans les 72 heures après en avoir pris connaissance[139]. La notification doit notamment décrire le contexte dans lequel la violation a eu lieu et les mesures qui ont été prises pour y remédier[140].

57. Exception à l'obligation de notification. Si la violation n'est pas susceptible de porter atteinte aux droits et libertés des personnes concernées, le responsable du traitement n'a

135 Article 5, § 1er, f), du Règlement ; voy. également, E. Thole, « How to handle data breaches from EU legal and practical perspective », in A. Grosjean (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 231-233.

136 Règlement (UE) n° 611/2013 du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.

137 Commission de la protection de la vie privée, Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données, n° 01/2013, 21 janvier 2013, p. 6.

138 Article 4, 12), du Règlement.

139 Article 33 du Règlement.

140 Article 33, § 3, du Règlement.

pas d'obligation de la notifier à l'autorité. Il devra néanmoins répertorier et documenter cette violation dans un registre, de façon à ce que les autorités de contrôle puissent évaluer le respect de l'article 33 relatif aux violations de données[141]. Le Règlement fait donc reposer sur le responsable du traitement la délicate question de savoir si une violation de données est susceptible de porter atteinte aux droits et libertés des individus, évaluation qui pourra *a posteriori* faire l'objet d'un contrôle de la part de l'autorité de contrôle.

58. Notification à la personne concernée. En outre, à moins que les données n'aient été rendues incompréhensibles (par exemple, grâce à la cryptographie) ou que le risque élevé ait été maîtrisé par le responsable du traitement, la violation de données devra également être communiquée dans les meilleurs délais aux individus concernés si elle engendre un risque élevé pour leurs droits et libertés[142]. Toutefois, si une telle communication devait demander des efforts disproportionnés, le responsable du traitement pourrait procéder à une communication publique ou recourir à tout autre moyen permettant d'informer les personnes concernées[143].

59. Obligation de notification du sous-traitant. Par ailleurs, si le sous-traitant n'a pas l'obligation de notifier une violation de données à l'autorité de contrôle contrairement au responsable du traitement, il doit néanmoins notifier les violations de données dont il est victime au responsable du traitement dans les meilleurs délais[144]. Bien souvent cette obligation sera déjà prévue dans les contrats de sous-traitance. Par contre, le responsable du traitement devra veiller à l'avenir à ce que ses sous-traitants lui transmettent les documents détaillant les violations de données qu'ils ont subies. En effet, une obligation de documentation de chaque violation de données pèse sur le responsable du traitement. Dès lors, il serait utile de revoir les contrats de sous-traitance et d'y ajouter, entre autres, cette obligation de documentation des violations de données à charge des sous-traitants. Cela aidera le responsable du traitement tant dans l'exercice de notification à l'autorité de contrôle que dans sa tenue de la documentation y relative.

60. Gestion des risques. En termes de gestion des risques, le but de cette notification est double. D'une part, elle permet aux personnes concernées de prendre les mesures utiles pour limiter le préjudice ou, à tout le moins, les effets néfastes que la violation de données peut engendrer. D'autre part, elle donne des informations à l'autorité de contrôle quant au nombre et aux circonstances dans lesquelles les violations de données se produisent et lui permet d'infliger des sanctions si les mesures techniques et organisationnelles adéquates n'ont pas été prises afin de protéger les données à caractère personnel.

2. Le nouveau régime de responsabilité (liability)

61. Régime prévu par la Directive. Dans le régime mis en place par la Directive, il incombe au responsable du traitement de respecter les principes généraux relatifs à la qualité des données comme l'indique son article 6, paragraphe 2. En cas de dommage causé à un individu, l'article 23 fait reposer l'entièreté de la responsabilité sur le responsable du traitement. C'est à ce dernier qu'il appartient de réparer le préjudice subi par la personne dont les données sont traitées. Il peut toutefois s'exonérer totalement ou partiellement de sa responsabilité s'il parvient à démontrer que le

141 Article 33, § 5, du Règlement.
142 Article 34, § 1er, du Règlement.
143 Article 34, § 3, c), du Règlement.
144 Article 33, § 2, du Règlement.

fait qui a occasionné le dommage ne lui est pas imputable[145].

Par ailleurs, la Directive est très succincte en ce qui concerne la responsabilité du sous-traitant. Elle se limite à dire que le sous-traitant qui accède à des données à caractère personnel ne peut les traiter que sur les instructions du responsable du traitement et que la relation entre ces deux parties doit être régie par un contrat ou par un acte juridique. L'article 17 précise en outre que le sous-traitant doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés. En résumé et comme l'indique le Groupe de l'article 29 dans son avis sur les notions de « responsable du traitement » et de « sous-traitant », la distinction opérée entre ces deux acteurs « sert avant tout à distinguer les intervenants qui assument la responsabilité du traitement de ceux qui ne font qu'agir pour le compte des premiers »[146]. On constate que la Directive attribue la responsabilité du respect des règles en matière de protection des données au responsable du traitement qui pourra, s'il le souhaite, intenter une action par la suite contre le sous-traitant si celui-ci n'a pas observé ses obligations contractuelles. Le but est *in fine* que les personnes dont les données à caractère personnel sont traitées puissent exercer effectivement leurs droits dans la pratique.

62. Difficulté pratique et nouveau régime. Dans la pratique, il est de plus en plus difficile de distinguer en quelle qualité agit chaque acteur, ceux-ci pouvant d'ailleurs revêtir une double casquette. Afin d'assurer aux personnes concernées la réparation de tout préjudice matériel ou immatériel causé par un traitement illicite, le Règlement a élargi les possibilités d'action à l'encontre de plusieurs acteurs vers lesquels les personnes concernées peuvent se tourner pour obtenir la réparation de leur dommage. En effet, l'article 82 du Règlement offre aux personnes concernées, et il s'agit là d'une innovation majeure, le choix d'intenter une action en responsabilité à l'encontre du responsable du traitement ou du sous-traitant.

Toutefois, alors que le responsable du traitement sera tenu responsable de tout préjudice résultant d'un traitement non conforme au Règlement, la responsabilité du sous-traitant est restreinte. Le Règlement limite, en effet, à deux hypothèses les cas dans lesquels il peut être tenu pour responsable du dommage causé[147]. Il pourra être tenu pour responsable lorsque, d'une part, il n'a pas respecté les instructions licites données par le responsable du traitement et, d'autre part, lorsqu'il n'a pas respecté les obligations que le nouveau Règlement met spécifiquement à sa charge. Dès lors, pour engager la responsabilité du sous-traitant il faudra prouver, en plus du dommage et de la non-conformité au Règlement, qu'il a commis un manquement à ses obligations légales spécifiques ou contractuelles[148]. Ce n'est que dans cette hypothèse qu'une action pourra être dirigée à son encontre.

Tant le responsable du traitement que le sous-traitant pourront s'exonérer de leur responsabilité s'ils démontrent que le dommage ne leur est nullement imputable.

145 Article 23, § 2, de la Directive.

146 Groupe de l'article 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, 16 février 2010, p. 6.

147 Article 82, § 2, du Règlement.

148 A. Myers, « Top 10 operational impacts of the GDPR: Part 7 – Vendor Management », 4 février 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management, consulté le 16 septembre 2016.

63. Responsabilité solidaire. Par ailleurs, le Règlement prévoit que chaque acteur du traitement responsable d'un dommage est tenu de réparer la totalité de celui-ci afin de garantir à la personne concernée une réparation effective[149]. Ainsi, en sus de prévoir une responsabilité directe du sous-traitant envers la personne concernée, le Règlement instaure une responsabilité solidaire entre co-responsables du traitement, entre sous-traitants, mais aussi entre le responsable du traitement et son sous-traitant[150]. L'article 82, § 4, du Règlement prévoit que lorsque plusieurs responsables du traitement ou sous-traitants, ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et lorsque leur responsabilité est engagée, chacun d'eux peut être tenu de réparer la totalité du dommage subi par la personne concernée. Celui qui aura réparé entièrement le dommage dispose d'un recours contre les autres responsables du traitement ou sous-traitants tenus pour responsables du dommage afin de récupérer auprès de chacun d'eux la part de la réparation correspondant à leur part de responsabilité dans le dommage[151].

On pourrait par ailleurs envisager que le sous-traitant ayant réparé le préjudice de la victime alors qu'une part de celui-ci incombait au responsable du traitement se retourne vers celui-ci pour obtenir un remboursement mais également pour réclamer des dommages et intérêts pour le préjudice que le sous-traitant aurait le cas échéant lui-même subi du fait d'une faute du responsable de traitement n'ayant pas rempli ses obligations en matière de protection des données.

Précisons encore que lorsque le sous-traitant fait lui-même appel à un sous-traitant pour mener des activités de traitement pour le compte du responsable du traitement et que ce sous-sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable vis-à-vis du responsable du traitement[152].

64. En pratique. À notre sens, cette nouvelle faculté va amener les acteurs intervenant dans le traitement de données à caractère personnel à repenser leurs relations contractuelles et la manière dont les responsabilités sont pour l'instant partagées. Le sous-traitant n'est plus considéré comme un simple exécutant, mais comme un acteur important devant endosser directement la responsabilité de ses actes en matière de traitement de données. De plus, il n'est pas à exclure que dans certains cas, le sous-traitant soit davantage connu que le responsable du traitement et dispose de ressources financières supérieures et qu'en conséquence les actions en responsabilité soient dirigées à son encontre plutôt qu'envers le responsable du traitement. Dès lors, à l'avenir, le sous-traitant devra faire preuve d'une vigilance accrue car, en plus de pouvoir faire l'objet d'une action directe, il n'a pas la mainmise sur l'entièreté de la légalité du traitement. Par exemple, le sous-traitant n'a aucune emprise sur le choix du fondement légal sur lequel repose le traitement, ce choix revenant exclusivement au responsable du traitement.

Au vu de ce qui précède, la négociation et la rédaction des contrats régissant la relation entre responsables du traitement et sous-traitants devraient s'avérer plus ardues, les

149 Article 82, § 4, du Règlement.

150 À ce sujet, voy. B. Van Alsenoy, *Regulating Data Protection – The allocation of responsibility and risk among actors involved in personal data processing*, PhD Thesis, August 2016, https://lirias.kuleuven.be/handle/123456789/545027, consulté le 5 septembre 2016.

151 Article 82, § 5, du Règlement.

152 Article 28, § 4, du Règlement.

dispositions devant être plus nombreuses et détaillées afin de régler précisément le partage de responsabilités en cas de violation du Règlement.

VI. RENFORCEMENT DE LA PROTECTION DES DROITS DES PERSONNES CONCERNÉES

65. Maîtrise renforcée sur les données. L'un des objectifs du Règlement est de conférer aux personnes dont les données à caractère personnel sont traitées une maîtrise effective sur celles-ci. À cette fin, le Règlement renforce l'ensemble des droits que la Directive reconnaissait aux personnes dont les données font l'objet d'un traitement, en clarifie certains et en ajoute de nouveaux. Toute personne concernée par un traitement de données à caractère personnel disposera dès la mise en application du Règlement d'un véritable arsenal de droits dont l'exercice devrait se trouver facilité.

A. Consolidation des droits existants

66. Le Règlement reprend l'ensemble des droits conférés par la Directive aux personnes dont les données à caractère personnel sont traitées, mais va plus loin en renforçant certains d'entre eux.

1. Obligation d'information accrue

67. Transparence accrue. Tout d'abord, le Règlement accroît la transparence des informations qui doivent être données par le responsable du traitement ainsi que des communications qui doivent être faites en réponse à l'exercice des droits de la personne concernée. Le texte édicte en outre les modalités d'exercice[153] de ces droits.

Sous l'empire de la Directive, certaines informations devaient déjà être portées à la connaissance des personnes concernées de manière systématique[154] et d'autres devaient l'être pour assurer la loyauté du traitement en raison des circonstances particulières et du contexte dans lequel s'inscrivait celui-ci[155].

À partir du 25 mai 2018, chaque responsable du traitement devra fournir à la personne concernée toute une série de nouvelles informations qu'il ne devait pas transmettre auparavant. Des mesures appropriées doivent par ailleurs être prises par le responsable du traitement pour fournir, par écrit ou par d'autres moyens (par voie électronique, par exemple), ces différentes informations[156].

En substance, les articles 13 et 14 du Règlement exigent qu'en sus des informations qui devaient déjà être fournies par le passé, deux types d'indications complémentaires soient données. D'un côté, des informations plus complètes sur le traitement doivent être communiquées[157] et de l'autre, le responsable du traitement doit fournir des renseignements additionnels quant aux modalités d'exercice de ses droits par l'individu[158].

Ces informations doivent être fournies de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information

153 Voy. article 12 du Règlement.

154 Article 10 de la Directive.

155 Article 10, c), de la Directive.

156 Article 12, § 1er, du Règlement.

157 Telles que, par exemple, la base juridique sur laquelle repose le traitement de données, la source d'où proviennent les données si celles-ci n'ont pas été collectées directement auprès de la personne concernée ou encore l'intention de transférer les données à caractère personnel vers un pays tiers ou à une organisation internationale.

158 À titre d'exemples, le droit d'introduire une réclamation auprès de l'autorité de contrôle doit être indiqué, l'existence des nouveaux droits à la portabilité des données et à la limitation du traitement doit également être mentionnée, ainsi que le droit de retirer son consentement à tout moment lorsque le traitement repose sur le consentement de la personne concernée.

destinée spécifiquement à un enfant[159]. Si par le passé, le responsable du traitement devait déjà communiquer à la personne concernée toute une série d'informations, force est de constater que celles-ci étaient rarement lues en raison notamment de la longueur et de la complexité des documents dans lesquels elles étaient insérées. Le législateur européen tente dès lors dans le Règlement de remédier à ce problème en mettant l'accent sur la transparence et la clarté avec lesquelles les informations doivent être mises à disposition. Cette préoccupation devra à l'avenir être prise d'autant plus au sérieux que le Règlement requiert que davantage d'informations soient fournies de manière systématique et circonstanciée[160]. L'utilisation d'icônes[161], par exemple, permettra de donner d'emblée aux individus une bonne visibilité sur le traitement.

Grâce à cette transparence accrue, les personnes concernées auront une meilleure vue sur le sort réservé à leurs données et sur les différents droits qui sont à leur disposition. En outre, le Règlement entend favoriser davantage l'exercice de ces droits en spécifiant les modalités d'exercice[162], ce qui n'était pas le cas dans la Directive.

68. Communication des informations. Dans la ligne de ce qui est prévu dans la Directive, les informations devant être communiquées et le moment auquel elles doivent l'être varient selon que les données ont été collectées directement auprès de la personne concernée ou non.

Lorsque les données à caractère personnel sont obtenues auprès de la personne concernée, les informations doivent être communiquées dès l'obtention des données[163]. Par contre, si les données n'ont pas été collectées auprès de la personne concernée, les informations doivent être communiquées dans un délai raisonnable, ne dépassant pas un mois, après leur obtention, ou dès la première communication avec la personne concernée ou avec un autre destinataire[164].

Cependant, si la personne concernée dispose déjà de l'ensemble de ces informations, il n'est pas nécessaire de les lui communiquer une nouvelle fois[165].

2. Droit d'opposition simplifié

69. Champ d'application limité. Le Règlement facilite l'exercice du droit d'opposition qui peut être mis en œuvre dans certaines hypothèses alors même que le traitement de données est licite. En effet, lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, ou en raison des intérêts légitimes du responsable du traitement ou d'un tiers, la personne dont les données sont traitées peut s'opposer au traitement. On notera qu'en cas de traitement basé sur le consentement de la personne concernée, c'est la possibilité du retrait du consentement[166] qui s'appliquera, rendant inutile l'exercice du droit d'opposition dans ce cas.

159 Article 12, § 1er, du Règlement.

160 Voy., par exemple, l'article 13, § 2, f), du Règlement qui requiert que la prise de décision automatisée soit communiquée, ainsi que les informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues pour la personne concernée.

161 Article 12, § 7, du Règlement.

162 Article 12 du Règlement.

163 Article 13, § 1er, du Règlement.

164 Article 14, § 3, du Règlement. Le considérant 61 mentionne que «la personne soit informée *du* moment auquel ces données à caractère personnel sont communiquées pour la première fois audit destinataire» (nous soulignons). Ce considérant est toutefois en contradiction avec l'article et ce sont les informations et non le moment qui doivent être communiquées à la personne concernée.

165 Article 13, § 4, du Règlement.

166 Article 7, § 3, du Règlement.

70. Renversement de la charge de la preuve. Aux termes de son article 14, la Directive exigeait que la personne concernée désirant s'opposer au traitement de ses données démontre «des raisons prépondérantes et légitimes tenant à sa situation particulière». Il fallait donc rapporter au responsable du traitement la preuve que l'opposition était justifiée pour obtenir l'arrêt du traitement. Le nouvel article 21 du Règlement simplifie l'exercice de ce droit car la personne concernée devra à l'avenir uniquement démontrer qu'elle a «des raisons tenant à sa situation particulière» pour obtenir la cessation du traitement de ses données. C'est au responsable du traitement qu'il incombera alors de prouver que ses intérêts légitimes et impérieux prévalent sur les intérêts de la personne concernée[167]. Durant le temps nécessaire au responsable du traitement pour faire la mise en balance des intérêts des parties, le traitement doit être limité, conformément à l'article 18, paragraphe 1er, d), du Règlement[168]. Le Règlement opère donc un renversement de la charge de la preuve au profit de la personne concernée. Ce changement doit être accueilli positivement car le responsable du traitement a à sa disposition davantage d'éléments que la personne concernée pour réaliser la mise en balance des intérêts.

Comme sous la Directive, si le traitement est réalisé à des fins de prospection, la personne concernée pourra s'y opposer sans justification aucune[169].

Toujours en vue de rendre l'exercice des droits effectif, le Règlement exige que le droit d'opposition soit explicitement porté à l'attention de la personne concernée et qu'il soit présenté clairement et séparément de toute autre information[170].

3. Consentement et droit de rétractation renforcés

71. Fin de la prédominance du consentement en tant que fondement? Un des fondements légaux sur lequel peut reposer le traitement de données à caractère personnel est le consentement de l'individu[171]. Ce fondement légal était jusqu'ici fréquemment utilisé par les responsables du traitement pour légitimer leurs activités de traitement de données. Une fois le Règlement d'application, le consentement ne devrait plus si facilement servir de fondement légal pour deux raisons majeures.

72. Qualité du consentement. Premièrement, le consentement sera plus difficile à obtenir car les règles en la matière seront désormais plus strictes[172]. Le législateur européen a voulu réagir à la multiplication des situations dans lesquelles un consentement de (très) mauvaise qualité servait de fondement légitime au traitement des données. En renforçant les exigences relatives au consentement, il a veillé à ce que, désormais, soit le responsable du traitement s'appuie sur un consentement de bonne qualité, soit il utilise une autre base de légitimité pour traiter ces données.

Le consentement doit être, comme sous l'empire de la Directive, libre, spécifique et éclairé[173]. Le Règlement précise, en outre, dans la définition qu'il donne au consentement, que celui-ci doit être univoque[174]. Le consentement sera

167 Considérant 69 du Règlement.
168 Sur la limitation du traitement, voy. *infra*, point 85.
169 Article 21, § 2, du Règlement.
170 Article 21, § 4, du Règlement.
171 Article 6, § 1er, a), du Règlement. Voy. *supra*, point 27.
172 Les exigences supplémentaires sur ce point s'inspirent des recommandations émises dans l'avis 15/2011 par le Groupe de l'article 29 sur la définition du consentement, 13 juillet 2011, WP 187.
173 Alors que le terme anglais «*informed*» utilisé dans la définition du consentement donnée dans la directive est maintenu dans la version anglaise du règlement, cet adjectif qui était traduit dans la version française de la directive par «informé» est cette fois traduit par «éclairé». Aucune différence de portée ne doit être attachée à ce nouveau terme.
174 Article 4, 11), du Règlement.

considéré comme éclairé lorsque la personne concernée a connaissance au moins de l'identité du responsable du traitement et des finalités du traitement auquel sont destinées les données à caractère personnel[175]. Il sera considéré comme ayant été librement donné uniquement si la personne concernée dispose d'une véritable liberté de choix ou est en mesure de refuser ou de retirer son consentement sans subir de préjudice[176]. À titre d'exemple, le consentement est présumé ne pas avoir été donné librement si l'exécution d'un contrat est suspendue au consentement pour le traitement de données qui ne sont pas nécessaires à ce contrat[177]. Le Règlement ajoute par ailleurs que le consentement doit se matérialiser par une déclaration ou par un acte positif clair[178]. Il peut ainsi se manifester par la détermination de certains paramètres techniques de sites web ou par le fait de cocher une case sur une page internet[179]. Le consentement peut également être donné par l'acceptation de termes et conditions, à condition que le consentement à ce traitement spécifique de données à caractère personnel soit clairement distinct des autres dispositions du document[180]. À l'inverse, le consentement ne peut découler du silence, de l'inactivité de l'individu ou encore de cases pré-cochées[181]. Cette précision dans le texte provient de la volonté de protéger les individus contre les consentements douteux, mais elle s'inscrit aussi dans la ligne de la nouvelle philosophie du Règlement. En effet, le principe d'*accountability* qui sous-tend le Règlement[182] requiert que le responsable du traitement soit en mesure de démontrer qu'il a bel et bien recueilli le consentement de la personne dont il traite des données. Dès lors, en pratique, il faudra veiller à se ménager la preuve qu'un tel consentement a bien été obtenu[183].

73. Exigence d'un consentement explicite. Par ailleurs, le Règlement est d'autant plus protecteur de l'individu lorsque les données qui font l'objet du traitement sont des données sensibles[184]. Dans ce cas, le responsable du traitement doit obtenir le consentement explicite de l'individu s'il choisit ce fondement pour légitimer son traitement[185].

En outre, le Règlement entend protéger davantage les mineurs dont les données à caractère personnel font l'objet d'un traitement. En effet, ceux-ci ont recours de plus en plus tôt à toutes les possibilités qu'offre internet. Par exemple, les écoles encouragent et optent de plus en plus pour l'utilisation de sites web à des fins éducatives. De plus, l'âge auquel les enfants commencent à utiliser internet, et avec lui ses réseaux sociaux, ne cesse de diminuer[186]. Au vu des risques significatifs que comportent ces traitements et afin de formaliser dans un texte les mesures protectrices pour les mineurs[187], un article spécifiquement dédié au consentement des enfants a été inséré dans le Règlement[188].

Dans le cadre de l'offre de services de la société de l'information, si le responsable du traitement

175 Considérant 42 du Règlement.
176 Considérant 42 du Règlement.
177 Article 7, § 4, et considérant 43 du Règlement.
178 Article 4, 11), du Règlement.
179 Considérant 32 du Règlement.
180 Considérant 42 du Règlement.
181 Considérant 32 du Règlement.
182 Voy. *supra,* point 25.
183 Article 7, § 1er, du Règlement.
184 Article 9, § 1er, du Règlement.
185 Article 9, § 2, a), du Règlement.
186 À ce sujet, voy. également K. Rosier, « Les réseaux sociaux et les jeunes : la Commission européenne exhorte à une protection renforcée de leur vie privée », *BSJ*, n° 460, 2011, www.lebulletin.be.
187 Par le passé, de grands sites web ont déjà signé un accord européen visant à améliorer la sécurité des mineurs qui utilisent les sites de socialisation en 2009, voy. le communiqué de presse de la Commission européenne du 10 février 2009 sur la « Socialisation sur internet : accord entre les grands sites par l'entremise de la Commission », http://europa.eu/rapid/press-release_IP-09-232_fr.htm?locale=fr.
188 Article 8 du Règlement.

envisage de traiter des données à caractère personnel se rapportant à un enfant sur la base de son consentement, il doit veiller à ce que l'enfant soit âgé de 16 ans pour que le traitement soit licite. Si l'enfant n'a pas encore atteint cet âge, le consentement devra être donné ou autorisé par le titulaire de la responsabilité parentale[189]. Dans ce cas, le responsable du traitement sera tenu de vérifier, dans la limite du raisonnable et en tenant compte des moyens technologiques disponibles, que la personne qui consent détient la responsabilité parentale à l'égard de l'enfant[190]. Les États membres ont néanmoins la faculté de réduire cette limite d'âge à un âge ne pouvant être inférieur à 13 ans[191]. Cette disposition accorde donc une protection spécifique aux enfants[192] en raison de leur vulnérabilité et en fonction de leur degré de maturité, conformément à ce que préconisait le Groupe de l'article 29[193]. Il va falloir développer des processus permettant de s'assurer de la qualité de la personne qui va accorder le consentement au nom de l'enfant. À cette fin, l'exemple américain du *Children's Online Privacy Protection Act* (COPPA) pourrait inspirer les États membres de l'Union[194]. Ce texte fournit notamment des indications intéressantes sur les différentes méthodes qu'il est possible d'utiliser pour obtenir le consentement des parents de l'enfant[195].

74. Validité des consentements existants. Qu'en est-il par ailleurs des consentements obtenus avant que le Règlement ne soit d'application ? Doivent-ils être donnés à nouveau ? La réponse à cette question dépendra d'une évaluation au cas par cas. En effet, un considérant du nouveau texte indique que « lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement (…) »[196]. En pratique, il faudra donc examiner si le consentement obtenu à l'époque a été donné par un acte positif clair, pour des finalités spécifiques et vérifier si le responsable du traitement est à même d'en rapporter la preuve[197]. Dans l'hypothèse inverse, un nouveau consentement devra être demandé aux individus dont les données sont traitées. Au vu des coûts qu'une telle démarche peut engendrer et des informations additionnelles que le Règlement enjoint de transmettre aux individus dont les données sont traitées, il serait peut-être judicieux de profiter de la transmission de ces nouvelles informations pour obtenir systématiquement un nouveau consentement conforme aux exigences du Règlement. Toutefois, le consentement devrait à l'avenir être de moins en moins utilisé pour légitimer le traitement de données à caractère personnel, et ce pour les raisons évoquées ci-avant et développées également dans les lignes qui suivent.

75. Rétractation du consentement. En effet, la seconde raison pour laquelle il devrait de moins en moins être recouru au consentement en tant que fondement légal du traitement de données est que le Règlement stipule que la personne dont les données sont traitées doit pouvoir à tout moment retirer son consentement aussi simplement qu'elle l'a donné[198]. La facilité avec laquelle l'individu va pouvoir retirer son consentement une fois que le Règlement

189 Article 8, § 1er, alinéa 1er, du Règlement.
190 Article 8, § 1er, alinéa 3 du Règlement.
191 Article 8, § 1er, alinéa 2 du Règlement.
192 Considérant 38 du Règlement.
193 Groupe de l'article 29, avis 2/2009 sur la protection des données à caractère personnel de l'enfant, 11 février 2009, WP 160.
194 www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.
195 À ce sujet, voy. § 312.5 du *Children's Online Privacy Protection Act*.
196 Considérant 171 du Règlement.
197 Considérant 42 du Règlement.
198 Article 7, § 3, du Règlement.

sera applicable fait peser un risque important sur le responsable du traitement : celui de se retrouver du jour au lendemain sans fondement légal légitimant à l'avenir son traitement de données à caractère personnel. Précisons que la licéité du traitement fondé sur le consentement avant que celui-ci ne soit retiré ne se verra pas compromise[199]. Toutefois, l'article 17 du Règlement prévoit au profit de la personne concernée un droit à l'effacement des données la concernant lorsqu'elle retire son consentement et lorsqu'il n'existe pas d'autre fondement juridique au traitement[200]. En conséquence, le responsable du traitement, lorsqu'il traite des données sur base du consentement, est susceptible non seulement de se retrouver inopinément sans fondement légal pour traiter ces données, mais de devoir également les effacer.

76. Portabilité des données collectées sur la base du consentement. Par ailleurs, si le traitement de données à caractère personnel repose sur le consentement de l'individu concerné ou sur un contrat auquel la personne concernée est partie, le responsable du traitement devra être davantage vigilant car cela ouvre la porte à l'exercice du droit à la portabilité des données pour l'individu concerné[201].

77. En pratique. Pour ces raisons et afin d'accroître la sécurité juridique, d'autres fondements tels que l'intérêt légitime du responsable du traitement pourraient être favorisés à l'avenir. À ce sujet, le fait que le Règlement oblige le responsable du traitement à communiquer aux personnes concernées ce qu'il considère comme étant son intérêt légitime contribuera par ailleurs à avoir un fondement légal solide car la personne aura une pleine connaissance de celui-ci dès le départ.

Finalement, à la lecture de l'article 7 du Règlement, il ressort que les nouvelles conditions applicables au consentement sont le fruit de longues discussions entre le Parlement, la Commission et le Conseil européens. Les deux premières institutions souhaitaient qu'un consentement explicite soit systématiquement demandé tandis que le Conseil européen s'y opposait fermement. *In fine*, un accord a été trouvé et ce compromis se traduit par un texte aux ambitions davantage protectrices de l'individu, même s'il est indéniable que l'exigence d'un consentement explicite dans tous les cas eût offert une meilleure protection des données.

B. Les « nouveaux droits »

En plus de renforcer les droits déjà existants sous l'empire de la Directive, le Règlement consacre de « nouveaux droits ». Il est fait usage de guillemets car, en réalité, les prémices de ces droits existaient déjà dans la Directive. Ainsi, le Règlement donne au droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (comme le profilage, par exemple), au droit à l'effacement (droit à l'oubli) et au droit à la limitation des données une nouvelle visibilité bien qu'il s'appuie sur des concepts déjà existants.

1. Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage

78. Définition. L'article 15 de la Directive abordait déjà la problématique des décisions individuelles automatisées en reconnaissant à toute personne « le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc. ».

199 Article 7, § 3, du Règlement.
200 Article 17, § 1er, b), du Règlement.
201 Article 20, § 1er, a), du Règlement. Voy. sur ce droit, *infra*, points 87 et s.

Le Règlement va plus loin et donne une définition de ce que recouvre le vocable « profilage »[202]. Il s'agit de « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique »[203]. Cette définition est très large et inclut notamment la publicité comportementale et la géolocalisation des individus.

79. Interdiction de principe. L'article 22 du Règlement reconnaît à la personne concernée « le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ». Le responsable du traitement ne peut donc *a priori* pas prendre de décision fondée uniquement sur du profilage et qui affecte la personne de manière significative ou qui produit des effets juridiques à l'encontre de celle-ci. Seront, à titre d'exemple, considérés comme tels, le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne ne nécessitant aucune intervention humaine[204].

80. Exceptions. Il y a toutefois trois situations dans lesquelles cette interdiction est levée[205]. Il s'agit tout d'abord du cas dans lequel la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne et le responsable du traitement. Deuxièmement, la décision automatisée est admise lorsqu'elle est autorisée par une disposition légale qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. Enfin, la personne concernée peut consentir explicitement à ce qu'une décision de ce type soit prise à son égard. Dans la première et la dernière hypothèse, le responsable du traitement devra au minimum permettre à la personne concernée d'obtenir l'intervention d'une personne, d'exprimer son point vue ainsi que de contester la décision automatisée et cela afin que ces droits et libertés soient sauvegardés[206].

Lorsque des décisions individuelles automatisées peuvent être prises, elles ne peuvent toutefois pas être fondées sur des données sensibles, à moins que la personne ait donné son consentement explicite au traitement ou que celui-ci soit nécessaire pour des motifs d'intérêt public important et que des mesures appropriées pour sauvegarder les droits et libertés de la personne soient prises[207]. Les décisions doivent également être fondées sur des données exactes et des algorithmes et inférences de qualité[208].

81. En pratique. Une fois le Règlement applicable, le profilage des individus sera certainement plus difficile à réaliser car peu d'entreprises pourront invoquer les deux premières exceptions pour échapper à l'interdiction de prendre de telles décisions. Elles devront donc obtenir le consentement explicite de la

202 Voy. également à ce sujet, Groupe de l'article 29, « Advice on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation », 13 mai 2013.
203 Article 4, 4), du Règlement.
204 Considérant 71 du Règlement.
205 Article 22, § 2, du Règlement.
206 Article 22, § 3, du Règlement.
207 Article 22, § 4, du Règlement.
208 A. Grosjean, « Le profilage : un défi pour la protection des données à caractère personnel », in A. Grosjean (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 294.

personne concernée qui ne sera pas évident à recueillir. En effet, en vertu du principe de transparence, le responsable du traitement doit informer la personne concernée de l'existence d'un profilage et des conséquences de celui-ci[209]. L'individu concerné doit également pouvoir s'opposer au profilage lié à des fins de marketing à tout moment et sans frais[210]. Ce droit d'opposition doit être explicitement et distinctement porté à son attention[211] et les données doivent être effacées sur le champ.

Par ailleurs, le Règlement ne précise pas davantage dans la Directive ce qu'il convient de considérer comme étant « une décision affectant la personne concernée de manière significative de façon similaire ». Il appartiendra là encore au responsable du traitement de déterminer au cas par cas si la décision automatisée qu'il envisage d'appliquer à une personne engendre de tels effets. À titre d'exemple, Alain Grosjean considère que « le profilage à des fins de marketing direct, la publicité comportementale, le courtage de données, la publicité basée sur la géolocalisation ou la publicité fondée sur le suivi des études de marché numérique (…) devraient être considérés comme affectant de façon significative leurs intérêts »[212].

Précisons finalement que lorsqu'un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union procède à un traitement de données lié au suivi du comportement de personnes s'y trouvant, il sera soumis au Règlement[213]. Tel sera notamment le cas lorsqu'une personne fait l'objet d'un suivi sur internet dans le but de prendre des décisions la concernant ou de prédire ses préférences, ses comportements et ses dispositions d'esprit par exemple[214]. Cela vise notamment l'hypothèse dans laquelle une société établie en Inde ou aux États-Unis par exemple traite les données de navigation sur la toile de citoyens européens dans le but d'étudier leurs comportements d'achat.

2. *Droit à l'effacement ou droit à l'oubli*

82. Un droit sous les feux des projecteurs médiatiques. Le droit à l'effacement est présenté dans le Règlement comme assimilé au « droit à l'oubli », notion qui a fait couler beaucoup d'encre et suscité de nombreux débats[215]. La Cour de justice a apporté, dans son désormais célèbre arrêt *Google Spain*[216], une forme de soutien à la Commissaire Viviane Reding qui avait multiplié les déclarations sur la nécessité de protéger les individus contre la mémoire éternelle d'internet en leur octroyant un droit à l'oubli qui serait consacré dans le Règlement alors en préparation. Ce faisant, la Cour avait montré qu'on pouvait faire découler un tel droit à l'oubli des éléments déjà existants du régime de protection des données, notamment du droit à l'effacement des données. Les auteurs du Règlement ont finalement opté pour une mise en évidence du droit à l'oubli en l'accolant expressément au droit à l'effacement repris à l'article 17.

209 Considérant 60 du Règlement.
210 Article 21, § 2, du Règlement.
211 Considérant 70 du Règlement.
212 A. Grosjean, « Le profilage : un défi pour la protection des données à caractère personnel », in A. Grosjean (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 302.
213 Considérant 24 et article 3, § 1er, b), du Règlement.
214 Considérant 24 du Règlement.
215 Voy. C. de Terwangne, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », in A. Grosjean (dir.), *Les enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 237-268.
216 C.J.U.E., 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) – Mario Costeja González*, C-131/12. Voy., parmi les très nombreux commentaires de cette décision majeure, E. Defreyne et R. Robert, « L'arrêt *Google Spain* : une clarification de la responsabilité des moteurs de recherche… aux conséquences encore floues », *R.D.T.I.*, 2015, n° 56, pp. 53-114, et les références citées.

Toute personne concernée peut, sans frais, faire effacer dans les meilleurs délais les données à caractère personnel qui se rapportent à elle « lorsque la conservation de ces données constitue une violation du présent règlement »[217].

Ce droit à l'effacement est en particulier valable lorsque les personnes concernées en viennent à retirer leur consentement donné antérieurement. Ce droit de changer d'avis et de revenir sur ce qu'on avait accepté sans peut-être envisager toutes les conséquences est particulièrement important dans le contexte d'aujourd'hui. Il est aussi précieux lorsqu'on en vient à regretter ce qu'on a exprimé ou diffusé grâce à l'interactivité du web. De telles situations sont malheureusement fréquentes quand l'expression est spontanée et impulsive, comme c'est souvent le cas sur les sites de réseaux sociaux, et spécialement quand celui qui s'exprime est jeune.

L'article 17 énonce d'autres hypothèses dans lesquelles s'applique le droit à l'oubli et à l'effacement : celle où il revient au responsable d'effacer les données qui ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, celle où la personne concernée s'oppose au traitement de ses données, celle qui se présente en cas de traitement illicite des données, traitement qui ne respecte donc pas les exigences du Règlement (les données sont, par exemple, incomplètes, non pertinentes ou excessives au regard de la finalité du traitement), celle où la loi impose l'effacement des données, et enfin celle où les données ont été collectées quand la personne était un enfant.

83. Le droit à l'effacement en aval. « Afin de renforcer le "droit à l'oubli numérique" »[218], l'article 17, paragraphe 2, étend le droit à l'effacement « de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les responsables du traitement qui traitent ces données à caractère personnel qu'il convient d'effacer tout lien vers ces données, ou toute copie ou reproduction de celles-ci. Ce faisant, ce responsable du traitement devrait prendre des mesures raisonnables, compte tenu des technologies disponibles et des moyens dont il dispose, y compris des mesures techniques, afin d'informer les responsables du traitement qui traitent les données à caractère personnel de la demande formulée par la personne concernée »[219].

Ceci a été présenté par certains commentateurs comme la réelle innovation du Règlement en ce qui concerne le droit à l'oubli. Pourtant le principe d'une obligation d'informer les personnes qui traitent des données controversées en aval du traitement initial est déjà présent dans la Directive[220]. On observe toutefois certaines divergences, la principale étant que cette obligation n'est attachée dans la Directive qu'à l'exercice du droit à l'effacement et non aux autres facettes du droit à l'oubli que sont le retrait du consentement et le droit d'opposition, alors que le Règlement élargit le devoir d'information en aval à l'ensemble de ces facettes, ce qui est particulièrement cohérent.

84. Un droit non absolu. Le droit à l'effacement et à l'oubli n'est bien sûr pas absolu et, dans une série de cas, notamment lorsque ce droit se heurte à l'exercice de la liberté d'expression ou à l'exécution d'une mission d'in-

217 Considérant 65 du Règlement.

218 *Ibid.*

219 *Ibid.*

220 L'article 12, c), de la Directive garantit que chaque personne concernée a le droit d'obtenir du responsable du traitement « c) la notification aux tiers auxquels les données ont été communiquées de […] tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné ».

térêt public, le traitement des données pourra se poursuivre.

3. *Le droit à la limitation du traitement*

85. Définition et effets. Le droit à la limitation du traitement des données est en fait une formulation autonome de ce qui était la troisième partie du droit reconnu à l'article 12, b), de la Directive : le droit d'obtenir « la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme (…) ». Le terme « verrouillage » a été pointé comme étant équivoque par les auteurs de la proposition de règlement[221] qui lui ont préféré l'expression « limitation du traitement », qui n'est malheureusement pas totalement plus claire… Au sens du Règlement, la limitation du traitement est « le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur »[222]. Toutefois, on ne voit pas d'emblée en quoi le marquage des données permet en lui-même de limiter le traitement.

Le second paragraphe de l'article 18 du Règlement spécifie quant à lui que la limitation du traitement engendre une interdiction de traiter les données (à moins d'avoir obtenu le consentement de la personne concernée), à l'exception de la conservation de celles-ci ou pour la constatation, l'exercice ou la défense de droits en justice entre autres. À part donc la conservation des données, aucune opération ne peut plus être réalisée sur ces données, sauf dans des circonstances très limitées. Dans la plupart des cas, ce droit à la limitation est un droit temporaire destiné à permettre des vérifications ou à conserver des données à des fins de preuve. Par exemple, une personne pourrait demander au responsable du traitement que ses données soient rendues inaccessibles sur son site web le temps de vérifier l'exactitude de celles-ci[223]. Le responsable du traitement rendra alors les données visées inaccessibles aux internautes le temps de résoudre la question.

86. Notification de la limitation. Précisons en outre que le responsable du traitement devra notifier à tous les destinataires des données que celles-ci ont fait l'objet d'une limitation, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés[224].

Par ailleurs, et c'est la véritable nouveauté par rapport au régime antérieur, à la demande de la personne concernée, le responsable du traitement est tenu de lui fournir des informations sur ces destinataires.

Ce droit vise en fait à régler temporairement la situation des parties dans l'attente de l'issue d'une contestation ou d'un procès par exemple. Une fois la situation réglée et avant que la limitation du traitement ne soit levée, le responsable du traitement en informe la personne[225].

C. Le véritable nouveau droit : le droit à la portabilité des données[226]

87. Nouvelles prérogatives. L'article 20 du Règlement reconnaît aux personnes dont les données à caractère personnel font l'objet d'un traitement un véritable nouveau droit : le droit à la portabilité des données. Celui-ci

221 Exposé des motifs de la proposition de règlement, p. 10 : « [L'article 17] intègre aussi le droit de limiter le traitement dans certains cas, en évitant le terme équivoque de "verrouillage" ».

222 Article 4, 3), du Règlement.

223 Article 18, § 1er, du Règlement et considérant 67 du Règlement.

224 Article 19 du Règlement.

225 Article 18, § 3, du Règlement.

226 Au moment d'écrire ces lignes, le Groupe de l'article 29 n'avait pas encore publié ses « Guidelines on the right to data portability », WP 242, adoptées le 13 décembre 2016, disponibles désormais à l'adresse http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

se subdivise en fait en deux prérogatives dont l'individu sera titulaire à l'avenir. D'une part, les personnes concernées ont le droit de recevoir les données à caractères personnel qu'elles ont fournies au responsable du traitement dans un format structuré, couramment utilisé et lisible par machine et d'autre part, elles ont le droit de transmettre ces données à un autre responsable de traitement. Néanmoins, l'étendue du droit à la portabilité des données est ostensiblement limitée lorsque plusieurs personnes sont concernées par un ensemble de données à caractère personnel. En effet, le quatrième paragraphe de l'article 20 stipule que « le droit [à la portabilité des données] ne porte pas atteinte aux droits et libertés des tiers ».

88. Conditions cumulatives d'exercice. L'exercice de ce droit est toutefois conditionné à la réunion simultanée de deux conditions. Premièrement, le traitement des données doit être fondé sur le consentement de la personne ou être nécessaire à l'exécution d'un contrat auquel elle est partie et, deuxièmement, il faut que le traitement ait été réalisé au moyen de processus automatisés[227]. En outre, ce n'est que lorsque cela est techniquement possible que le responsable du traitement devra transmettre lui-même, à la demande de la personne concernée, les données directement à un autre responsable du traitement[228].

89. Interopérabilité. Afin que ce droit puisse être exercé de manière effective, il faudra que les responsables du traitement s'accordent sur le choix de formats interopérables pour transférer les données. Un considérant indique néanmoins que le droit à la portabilité des données « ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles », ce qui n'est pas sans susciter l'interrogation. Cela risque en effet de constituer une barrière considérable à l'exercice effectif du droit à la portabilité des données[229].

90. Notion de « données fournies ». Au surplus, seules les données fournies par la personne au responsable du traitement sont concernées par l'exercice de ce droit. Le Règlement ne donne aucune indication sur l'interprétation qu'il convient de faire des termes « données fournies ». Doit-on interpréter cette notion strictement et la limiter aux données procurées par l'individu ou peut-on lui reconnaître une portée plus large[230] ? Les données fournies passivement par le biais de cookies ou encore les données créées par le responsable du traitement sur la base des données fournies par la personne (*profiling*, *credit score*, …), par exemple, sont-elles visées par le droit à la portabilité des données ? Le doute est permis quant à la réponse à donner à cette question. En effet, l'adresse IP, l'historique de navigation, les données de géolocalisation sont autant d'exemples de données générées passivement par l'individu lors de sa navigation, mais qu'il ne fournit pas en tant que telles. Le second exemple, impliquant un apport du responsable du traitement, pose quant à lui des questions en termes de protection du savoir-faire et du secret des affaires. Étendre la portée du droit à la portabilité des données aux données développées par le responsable de traitement grâce aux données fournies par la personne reviendrait, en effet, dans bien des cas à porter atteinte à ces droits et il ne nous semble dès lors pas que ce nouveau droit à la portabilité des données doive recevoir une telle portée. Par exemple, comment un réseau

227 Article 20, § 1er, a) et b), du Règlement.

228 Article 20, § 2, du Règlement.

229 Considérant 68 du Règlement.

230 Voy. not. sur le sujet, P. Valcke et J. Verschakelen, « Dataportabiliteit en digitale (mensen-)handel », *N.J.W.*, 9 avril 2014, pp. 298-300.

social, va-t-il faire face à cette obligation de transférer l'ensemble des données qui lui ont été fournies par l'utilisateur à un autre réseau social ? Cela pose indéniablement des questions en matière de propriété intellectuelle et de droit de la concurrence. Il est à noter que le droit d'accès[231] permettra néanmoins à la personne concernée d'obtenir du responsable du traitement l'accès aux données à caractère personnel la concernant ainsi qu'une copie de celles-ci[232]. Ainsi, on pourrait imaginer qu'en vertu de ce droit, la personne ait accès au profil de consommation établi par le responsable du traitement grâce au profilage par exemple.

Destiné à favoriser la mobilité des clients dans l'environnement en ligne, le droit à la portabilité des données constitue une révolution en matière de protection des données et suscite des interrogations quant à sa mise en œuvre. Il renforce indéniablement l'emprise qu'ont les individus sur leurs données. Reste à voir comment l'exercice de ce droit se mettra en place en pratique et comment les questions qu'il soulève seront résolues.

D. Multiplication des voies de recours

91. Types de recours. Le Règlement entend renforcer les voies de recours mises à disposition des personnes qui estiment que les droits que leur confère le Règlement sont violés. En substance, trois types de recours seront ouverts aux personnes concernées.

Premièrement, toute personne concernée pourra introduire une réclamation auprès de l'autorité de contrôle de l'État membre dans lequel se trouve sa résidence principale, son lieu de travail ou dans lequel la violation du Règlement aurait été commise[233]. Une telle procédure pourra déboucher sur l'imposition d'importantes amendes administratives par l'autorité de contrôle[234].

Deuxièmement, en cas d'inaction de l'autorité de contrôle dans un délai de trois mois ou de désaccord avec une décision juridiquement contraignante prononcée par l'autorité de contrôle, la personne concernée peut introduire un recours devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie[235].

Enfin, comme rappelé *supra*[236], l'article 82 du Règlement stipule que « toute personne (…) a le droit d'obtenir du responsable du traitement *ou* du sous-traitant réparation du préjudice subi » en justice (nous soulignons). Le choix de pouvoir intenter une action contre le responsable du traitement ou contre le sous-traitant responsable du dommage constitue l'une des innovations majeures du Règlement. Cette action pourra être introduite devant les tribunaux de l'État membre dans lequel la partie qui traite les données a un établissement ou au lieu de résidence habituelle du demandeur[237].

92. Action collective. Par ailleurs, si la personne concernée ne souhaite pas introduire elle-même sa réclamation ou son action en justice, elle aura à l'avenir la faculté de mandater un organisme, une organisation ou une asbl valablement constituée selon le droit national, dont les objectifs statutaires sont d'intérêt public et qui est actif/ve dans le domaine de la protection des droits et libertés des personnes concernées pour ce faire[238]. Les États membres peuvent, s'ils le souhaitent, accorder à de telles structures le droit d'obtenir la réparation du préjudice subi au nom de la personne concernée. Ils peuvent par ailleurs

231 Article 15 du Réglement.
232 Article 15, § 3, du Règlement.
233 Article 77, § 1er, du Règlement.
234 À ce sujet, voy. *infra*, point 95.
235 Article 78 du Règlement.
236 Voy. points 61 et s.
237 Article 79 du Règlement.
238 Article 80, § 1er, du Règlement.

prévoir la faculté pour ces associations d'introduire une réclamation ou un recours juridictionnel sans recevoir de mandat d'un individu si elles considèrent que les droits reconnus aux individus par le Règlement ont été enfreints[239]. Grâce à cet article 80, des organismes ou associations ayant pour objet la protection de la vie privée ou la défense des intérêts des consommateurs, par exemple, pourront introduire des recours collectifs de leur propre initiative, indépendamment d'un mandat. Si la Directive prévoyait déjà la possibilité pour une association représentant la personne concernée de saisir l'autorité de contrôle d'une plainte[240], cette faculté n'avait pas été transposée en tant que telle à l'article 31 de la loi du 8 décembre 1992, celui-ci exigeant que la plainte soit datée et signée par le plaignant lui-même.

À l'avenir, le Règlement étant d'application directe, les personnes résidant sur le territoire belge disposeront d'un pouvoir effectif de mandater l'un ou l'autre organisme pour mener à bien leur réclamation ou action relative à une violation du Règlement. Le nombre d'actions intentées en la matière devrait considérablement augmenter eu égard notamment au fait que les violations de cette réglementation toucheront, en raison de leur spécificité, un nombre important de personnes[241]. On pense, par exemple, aux fuites de données portées à la connaissance du public[242] contre lesquelles une action collective pourra être intentée dans le futur. Le recours à de telles actions collectives permettra également de répartir les coûts, souvent importants, de la procédure. Les nouvelles dispositions relatives aux voies de recours devraient donc contribuer à accroître l'effectivité des droits des personnes concernées et à augmenter le nombre de réclamations et de recours intentés en matière de protection des données à caractère personnel. Cette constatation combinée au montant plus élevé des amendes constitue inéluctablement un incitant au respect des dispositions du Règlement.

VII. ACCENTUATION DU RÔLE DES AUTORITÉS DE CONTRÔLE ET RENFORCEMENT DES SANCTIONS

93. Plus de contrôle pour plus d'effectivité. Il ne faut pas se faire d'illusion. Sans risque de réelles sanctions en cas de non-respect, une telle réglementation a peu de chance d'être effective. Ces dernières années l'ont prouvé. C'est essentiellement la multiplication des actions des autorités de contrôle nationales, notamment vis-à-vis de grandes entreprises d'outre-Atlantique, qui a fait progresser la protection des données sur le terrain de la visibilité, pas seulement dans les media mais également dans les prétoires. En témoigne le nombre exponentiel de décisions de la Cour de justice rendues à propos de la Directive depuis une dizaine d'années.

Les nouvelles dispositions du Règlement consacrent des pouvoirs accrus des autorités de contrôle, des mécanismes de coordination et de répartition des actions et compétences des différentes autorités nationales et des sanctions plus lourdes en cas de non-respect du Règlement.

Dans le cadre de cette contribution, nous n'entrerons pas dans le détail de ces modifications qui, pour la plupart appellent une mise en place de nouvelles règles tant au niveau des autorités de contrôle qu'au niveau européen. Une analyse exhaustive est donc prématurée dès

239 Article 80, § 2, du Règlement.

240 Article 28, § 4, de la Directive.

241 T. Van Canneyt et G. Goossens, «The general data protection regulation: 10 things company lawyers should know», *C.J.*, 2016/1, p. 11.

242 Telles que la fuite de données ayant touché 700.000 clients de la SNCB en 2012 ou celle dont ont été victimes les 32 millions d'utilisateurs du site Ashley Madison en 2015.

lors que le chantier est encore en cours. Nous nous limiterons donc à pointer quelques-uns des aspects qui nous paraissent les plus importants des changements qui interviendront.

De manière générale, les autorités de contrôle voient leurs pouvoirs en matière de guidance dans l'application de la réglementation[243] et de mesures « correctrices » en cas de mauvaise application de celle-ci élargis. Il s'agit selon nous des pôles au travers desquels une effectivité de la réglementation doit être réalisée : aider les acteurs concernés, aussi bien les personnes concernées que les responsables du traitement/sous-traitants, à comprendre ce qu'implique le respect de la réglementation et sanctionner en cas de non-respect de celle-ci.

94. Le rôle de guidance. Il est évident que les autorités de contrôle ont un rôle à jouer pour fournir des indications sur la manière dont le Règlement doit être appliqué d'autant que de cette réglementation est assez complexe et repose largement sur des pondérations à faire au cas par cas. On notera que le Règlement impose aux autorités de « favoriser la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement »[244]. Conscientiser et informer les citoyens est essentiel. Un citoyen non informé de ses droits ne les fera pas valoir.

Le considérant 132 précise que les activités de sensibilisation devraient comprendre des mesures spécifiques destinées aux responsables du traitement et aux sous-traitants, y compris les micros, petites et moyennes entreprises. Il n'y a toutefois pas d'obligation de donner sur demande un avis au responsable du traitement ou au sous-traitant sur la manière d'appliquer la réglementation à un cas particulier, hormis dans des hypothèses spécifiques (telle une analyse d'impact qui révélerait des risques élevés, par exemple[245]). Pas de « *ruling privacy* » donc.

95. Le rôle de gendarme de la protection des données. C'est dans le cadre des mesures dites correctrices qu'intervient la « guidance » *ad hoc* de l'autorité. En sus de ses pouvoirs d'enquête[246], cette dernière peut, entre autres, (1) avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement ou encore (2) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du Règlement, le cas échéant, de manière spécifique et dans un délai déterminé[247].

Concernant les sanctions, l'autorité de contrôle peut adopter des mesures correctrices dans un catalogue assez large qui compte onze mesures énoncées à l'article 58, paragraphe 2, du Règlement. Les autorités de contrôle pourront, par exemple, imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement[248].

Parmi ces mesures, on retiendra également l'imposition d'une amende administrative, le cas échéant en complément d'autres mesures correctrices. Il s'agira d'une nouvelle compétence pour la Commission de la protection de la vie privée, cette dernière n'ayant à ce jour que la possibilité de dénoncer au Parquet les infractions à la loi dont elle a connaissance[249]. On ignore encore quelles seront les modalités concrètes de la réorganisation de la Commission pour intégrer notamment cette compétence, mais il est d'ores et déjà acquis qu'une

243 Voy. article 57 du Règlement.
244 Article 57, § 1er, b), du Règlement.
245 Article 57, § 1er, l), et article 58, § 3, a), du Règlement ; voy. *supra*, points 45 et s.
246 Voy. article 58, § 1er, du Règlement.
247 Article 57, § 2, a) et d), du Règlement.
248 Article 58, § 2, f), g) et i), du Règlement.
249 Article 32, § 2, de la loi du 8 décembre 1992.

voie de recours juridictionnel contre ses décisions devra être prévue[250].

96. Des sanctions plus dissuasives. Un autre point qui mérite d'être souligné est que le Règlement a pris le parti de prévoir des sanctions qui pourront s'avérer extrêmement lourdes financièrement. Pour les manquements les plus graves, l'amende peut aller jusqu'à 20.000.000 euros ou, pour une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial de l'exercice précédent[251]. Ceci devrait donner à réfléchir lorsqu'il sera question du degré de priorité à donner aux aspects de la protection des données d'un projet.

97. La répartition des compétences entre autorités de contrôle. Enfin, de nouvelles règles associées à de nouveaux concepts apparaissent pour régler la répartition des compétences des autorités de contrôle ainsi que la coopération entre elles lorsqu'une même activité affecte ou implique plusieurs territoires.

La compétence de l'autorité de contrôle est territoriale et dépendra du siège de l'« établissement principal » du responsable du traitement ou sous-traitant concerné. Cette nouvelle notion tente tant bien que mal d'anticiper les différents cas de figure qui peuvent se présenter en cas de pluralité d'établissements associés à un même traitement[252]. La notion définie à l'article 4, 16), du Règlement combine des critères alternatifs. Pour le responsable du traitement, il s'agira de l'établissement du responsable du traitement dans l'Union qui prend les décisions quant aux finalités et moyens de traitement et a le pouvoir de les faire appliquer[253], ou à défaut le lieu de l'administration centrale du responsable du traitement dans l'Union. Pour le sous-traitant, c'est du lieu de son administration centrale dans l'Union ou, à défaut, du lieu où se déroule l'essentiel de ses activités dont il faudra tenir compte.

Dans le cas d'un « traitement transfrontalier »[254], à savoir celui qui a lieu dans le cadre des activités de plusieurs établissements d'un responsable du traitement ou d'un sous-traitant dans différents États de l'Union ou qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres, une autorité de contrôle sera désignée comme « chef de file » et sera amenée à coopérer avec les autres autorités concernées[255] dans l'exercice de ses pouvoirs et missions relatifs au traitement concerné[256]. L'objectif est certainement de favoriser une

250 Article 58, § 4, du Règlement.

251 Article 83 du Règlement.

252 Voy. les inquiétudes quant aux difficultés pratiques en cas de groupe d'entreprises notamment évoquées dans l'avis du Contrôleur européen de la protection des données sur le paquet de mesures pour une réforme de la protection des données, 7 mars 2012, www.edps.europa.eu, p. 20.

253 Ou dans le cadre d'un groupe d'entreprise, l'entreprise qui contrôle les autres membres du groupe (considérant 36 du Règlement).

254 L'article 4, 23), du Règlement définit le « traitement transfrontalier » comme étant : « a) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ; ou b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres ».

255 C'est-à-dire au sens de l'article 4, 22), du Règlement, une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que (1) le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève, (2) des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ; ou (3) une réclamation a été introduite auprès de cette autorité de contrôle.

256 Voy. en particulier l'article 60 du Règlement qui définit les modalités de cette coopération.

cohérence dans les actions des autorités de contrôle mais également, pour les responsables du traitement actifs dans plusieurs États membres, d'avoir une autorité de contrôle comme interlocuteur, et non plusieurs (*one-stop shop*)[257].

VIII. FLUX TRANSFRONTIÈRES DE DONNÉES

98. Continuité du régime des flux transfrontières de données. Le Règlement ne révolutionne pas le régime des flux transfrontières de données, même s'il apporte d'intéressantes précisions et compléments. Le chapitre V reprend les règles qui régissaient la matière depuis 1995 en intégrant les instruments légaux qui ont fait leur apparition depuis lors pour assurer une protection aux données qui franchissent les frontières de l'Union européenne. Ainsi, les transferts de données hors de l'espace de protection européen (c'est-à-dire hors de l'UE et de l'Espace économique européen) sont interdits à moins que le pays de destination des données n'ait été reconnu comme assurant une protection adéquate aux données, ou que l'émetteur des données n'offre lui-même une protection adéquate par le biais de garanties appropriées telles des clauses contractuelles ou des règles d'entreprises contraignantes[258], ou enfin qu'une dérogation trouve à s'appliquer[259].

99. Absence de définition de la notion de « transfert ». On regrettera que le législateur n'ait pas saisi l'occasion de l'élaboration du Règlement pour définir la notion de « transfert » qui aurait certes mérité une clarification[260]. Les auteurs du texte auraient pu reprendre la définition proposée par le Contrôleur européen à la protection des données (l'EDPS) dans son *position paper* sur la question des transferts de données. Le transfert est défini en ces termes : « la communication, la divulgation ou la mise à disposition de données à caractère personnel par un expéditeur relevant du règlement et conscient que le ou les destinataires y auront accès ou agissant dans cette intention »[261]. Dans le même sens, le projet de Rapport explicatif de la Convention 108 révisée précise que « un transfert de données intervient lorsque des données à caractère personnel sont communiquées ou mises à disposition d'un destinataire relevant de la juridiction d'un autre État ou d'une autre organisation internationale »[262].

100. Décisions d'adéquation. Désormais, il n'appartiendra plus qu'à la Commission

257 Dans le même sens, le Règlement consacre le mécanisme des règles d'entreprise contraignantes qui permettent, en matière de flux de données au sein d'un même groupe d'entreprises vers des pays tiers n'assurant pas un niveau de protection adéquat, de faire valider lesdites règles pour tout le groupe auprès d'une seule autorité de contrôle, nonobstant le fait que plusieurs entreprises concernées soient, le cas échéant, situées sur différents territoires de l'Union (*cfr* article 47 du Règlement).

258 Ces règles sont couramment évoquées sous leur appellation anglaise : *binding corporate rules* (BCR). Elles sont définies à l'article 4, 20), du Règlement.

259 Articles 44 et suivants du Règlement.

260 Dans le même sens, voy. Contrôleur européen de la protection des données, avis du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, p. 21, point 108, disponible à l'adresse : https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_FR.pdf. Voy. également, C. Gayrel et R. Robert, « Proposition de règlement sur la protection des données. Premiers commentaires », *J.D.E.*, 2012, p. 179.

261 Contrôleur européen de la protection des données, « Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne », Document d'orientation, 14 juillet 2014, p. 7, disponible à l'adresse : https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_FR.pdf.

262 Conseil de l'Europe, Projet de rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n° 108, version du 5 septembre 2016, § 98.

européenne de se prononcer sur le caractère adéquat du niveau de protection offert par un régime, que ce régime soit celui d'un pays tiers, d'un territoire ou d'un secteur dans un pays tiers, ou encore d'une organisation internationale. Tirant les leçons de ce que la Cour de justice a proclamé dans son retentissant arrêt *Schrems*[263], les auteurs du Règlement ont ajouté, dans le considérant 104, la précision que ce qui est évalué, ce sont les garanties offertes par le régime tiers « pour assurer un niveau adéquat de protection *essentiellement équivalent à celui qui est garanti dans l'Union* »[264]. Le régime juridique évalué doit donc présenter un niveau de protection « essentiellement équivalent » au niveau européen, ce qui pourrait se traduire par un niveau très comparable sans être pour autant identique au niveau européen. Ce qui est recherché à travers la notion de protection « essentiellement équivalente » c'est la continuité du niveau élevé de protection en cas de transfert de données vers un pays tiers[265].

Pour évaluer le caractère adéquat de la protection offerte, la Commission est invitée à tenir compte d'une série de critères qui sont à présent énoncés dans le texte même du Règlement[266]. Ces critères comprennent ceux appliqués jusqu'ici et issus principalement du document de travail du Groupe de l'article 29 sur les flux transfrontières et la notion de protection adéquate[267], auxquels s'ajoutent des critères liés au respect de l'état de droit, au respect des droits de l'homme et des libertés fondamentales, à la législation relative à la sécurité publique, la défense, la sécurité nationale et le droit pénal. À cela a été ajouté en fin de parcours législatif un critère découlant directement de l'arrêt *Schrems*[268] : l'accès des autorités publiques aux données à caractère personnel.

C'est encore l'arrêt *Schrems*, qui a vu la Cour invalider des années plus tard une décision reconnaissant le niveau adéquat de la protection offerte par un système de protection (le système du *Safe Harbour* impliquant les États-Unis), qui a conduit les auteurs du texte à insérer l'obligation pour la Commission d'assurer une veille permanente des conditions entourant ses décisions d'adéquation[269], ainsi que de prévoir un examen périodique (au moins tous les 4 ans) des évolutions qui seraient apparues dans un régime juridique tiers ayant fait l'objet d'une décision d'adéquation[270], examen qui pourrait déboucher sur l'abrogation ou la suspension de la décision d'adéquation[271].

101. Garanties appropriées. En l'absence de décision d'adéquation du régime juridique d'un État tiers, on pourra y transférer des données si le responsable du traitement ou le sous-traitant compensent l'absence de protection satisfaisante en prévoyant eux-mêmes des garanties appropriées[272]. Nouvel apport de la jurisprudence *Schrems*, le texte ajoute la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives, « ce qui comprend le droit d'engager un recours administratif ou juridictionnel effectif et d'introduire une action en réparation, dans l'Union ou dans un pays tiers »[273].

263 C.J.U.E. (gr. ch.), 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14.
264 Nous soulignons.
265 C.J.U.E., arrêt *Schrems*, précité, points 172 et 173.
266 Article 45 du Règlement.
267 Voy. le document de travail du Groupe de l'article 29, « Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données », WP 12, adopté le 24 juillet 1998, disponible à l'adresse : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_fr.pdf.
268 C.J.U.E. (gr. ch.), 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14.
269 Article 45, § 4, du Règlement.
270 Article 45, § 3, du Règlement.
271 Article 45, § 5, du Règlement.
272 Article 46 du Règlement et considérant 108.
273 Considérant 108.

Au-delà de ce qui est évoqué ci-dessus, les garanties appropriées peuvent prendre la forme d'un instrument juridique contraignant entre autorités publiques, d'un code de conduite ou d'un mécanisme de certification, tous deux assortis d'un engagement contraignant pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer ces garanties[274].

102. Dérogations. Les cas dans lesquels la Directive admettait les transferts de données vers un pays n'offrant pas de protection adéquate sont repris dans le Règlement[275]. Des changements sont apportés dans cette liste sur deux seuls points : le consentement qui peut être donné par la personne concernée pour autoriser un transfert de ses données doit à présent être explicite plutôt qu'indubitable, la personne concernée devant avoir été informée des risques liés à l'absence de protection des données au-delà de la frontière. Et les cas d'autorisation d'un transfert pour la sauvegarde des intérêts vitaux de la personne concernée sont élargis aux intérêts vitaux d'autres personnes. Il est précisé que cette hypothèse d'exception est valable « lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ». Les autres cas sont repris sans véritable modification : les transferts nécessaires à la conclusion ou l'exécution d'un contrat, ceux nécessaires pour des motifs importants d'intérêt public (comme les échanges entre autorités fiscales ou douanières, les transferts pour des questions de santé publique ou ceux liés à la lutte contre le dopage), ou pour la défense de droits en justice et enfin ceux effectués à partir de registres publics.

Le Règlement ajoute un cas d'exception tout à fait nouveau et passablement interpellant. Il s'agit de transferts qui ne peuvent s'appuyer sur une décision d'adéquation du régime juridique destinataire des données ni ne sont encadrés par des garanties appropriées ou des règles d'entreprise contraignantes (*Binding Corporate Rules* – BCR). Lorsqu'aucune des exceptions évoquées ci-dessus ne peut jouer, il sera quand même possible d'envoyer des données hors des frontières si l'on est en présence d'un transfert n'ayant pas de caractère répétitif, ne touchant qu'un nombre limité de personnes et qui est nécessaire pour les intérêts légitimes impérieux poursuivis par le responsable du traitement, prévalant sur les intérêts et droits fondamentaux des personnes concernées. Il importe que le responsable du traitement évalue toutes les circonstances du transfert, en tenant compte de la nature des données, de la finalité et de la durée du traitement et de la « situation dans le pays tiers »[276]. Il faut aussi que le responsable offre, à partir de cette évaluation, des garanties appropriées (qui ne sont donc pas du même niveau que les garanties appropriées contenues dans des clauses contractuelles ou BCR[277]) et qu'il informe l'autorité de contrôle et les personnes concernées du transfert et des intérêts impérieux en jeu[278]. Il semble, à la lecture du considérant 113, que le législateur européen ait eu notamment en tête les transferts à des fins de recherche scientifique ou historique ou à des fins statistiques, mettant en jeu le progrès des connaissances pour lequel la société a des attentes légitimes (mais qui ne relèvent pas d'un intérêt public important, sinon, ils seraient couverts par l'exception prévue à l'article 49, paragraphe 1er)…

274 Article 46, § 2 ; voy. également, § 3, du Règlement.

275 Article 49 du Règlement.

276 Considérant 113.

277 La version anglaise échappe à cette formulation paradoxale en ne reprenant pas ici le terme « *appropriate safeguards* » qu'elle réserve à l'article 46, mais « *suitable safeguards* » qui marque bien qu'il ne s'agit pas du même niveau de garanties.

278 Article 49, § 1er, alinéa 2, du Règlement.

IX. CONCLUSION

Le texte du Règlement est dense et nous sommes loin d'avoir pu explorer toutes les questions qu'il peut susciter. La confrontation du texte à des applications en pratique sera sans nul doute source de nouveaux questionnements et de réflexions.

Nous l'avons souligné, la nouvelle réglementation est ambitieuse et entend permettre une plus grande effectivité du respect des principes de protection des données, en tenant compte notamment du caractère plus globalisé des possibilités de traitements à la fois à l'échelle internationale et dans l'ampleur des traitements rendus possibles par la technologie.

Nous avons mis en exergue certaines lignes de force du Règlement. Nous retiendrons en particulier une responsabilisation accrue des différents acteurs. Une approche dynamique et proactive est désormais explicitement exigée des responsables du traitement pour anticiper et réduire les risques en matière de protection des données. Le sous-traitant, grand perdant de la réforme, reste confiné dans un rôle d'exécutant tout en endossant une responsabilité plus importante tant vis-à-vis du responsable de traitement que des personnes concernées et des autorités de contrôle. Les personnes concernées voient leurs droits renforcés pour leur assurer une plus grande maîtrise de leurs données. Les autorités de contrôle sont dotées de pouvoirs de sanction élargis, avec l'espoir qu'elles en feront usage pour assurer une plus grande effectivité de la réglementation.

Nous ne pouvons manquer de noter à cet égard les sanctions en termes d'amendes, notamment, qui se veulent plus dissuasives et qui posent question. Au-delà de savoir quels chiffres d'affaires seront pris en compte dans le cas de groupes de sociétés, on peut s'interroger sur le principe même des sanctions extrêmement lourdes et se demander s'il est conciliable avec l'exigence de prévisibilité des règles à respecter. En effet, le respect du Règlement appelle sur bien des points une appréciation au cas par cas et une pondération qui laisse à tout le moins place à la discussion. Les actes d'exécution de la Commission, des avis du Comité européen et des *guidelines* des autorités nationales seront certainement très attendus pour créer davantage de sécurité juridique.

Par ailleurs, si le choix d'un Règlement atteste de la volonté d'harmoniser les règles en matière de protection de données à caractère personnel au niveau européen, force est de constater que la réglementation ne sera pas totalement harmonisée. Le législateur européen a laissé une certaine marge de manœuvre aux États membres, leur permettant d'introduire un certain nombre de spécificités au niveau national. Par ailleurs, bien que des règles de coopération entre les autorités nationales de contrôle aient été définies pour une gestion cohérente des contrôles et des sanctions, l'ancrage local du contrôle subsiste avec également des différences qui peuvent se créer dans la manière d'appréhender la protection des données d'un État à l'autre.

À l'agenda, les actes délégués et les *guidelines* du Groupe de l'article 29 pour préparer l'entrée en application du Règlement mais également l'adaptation de la législation belge sont attendus des praticiens d'ici mai 2018.