Le règlement européen relatif à la protection des données à caractère personnel

De Terwangne, Cécile; Rosier, Karen; Losdyck, Bénédicte

Published in:
Journal de droit européen

Publication date:
2017

Document Version
le PDF de l'éditeur

Analyse

Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ?

Cécile de Terwangne, Karen Rosier et Bénédicte Losdyck(*)

- **Le nouveau règlement général sur la protection des données personnelles vise à protéger les individus dans la société connectée d'aujourd'hui**
- **Il redessine les obligations de ceux qui traitent des données (responsabilité, protection contre les violations de données, désignation de spécialistes en la matière, etc.) et les droits accordés aux individus (droit à l'information, droit à l'oubli, droit à la portabilité des données, etc.)**
- **Il ambitionne une plus grande effectivité de la protection que la directive 95/46 qu'il remplace et dispose de plusieurs armes pour y parvenir**

Introduction

Une véritable révision de la réglementation. — Après quatre ans de discussions soutenues et de négociations tendues, le législateur européen a adopté le 27 avril 2016 le règlement général sur la protection des données (R.G.P.D., ci-après le « règlement »)[1]. Ce texte vient en réponse à la nécessité qui s'était fait jour de réviser la directive 95/46/CE[2] (ci-après la « directive ») qui réglementait depuis 1995 la matière de la protection des données à caractère personnel et qui n'avait pu anticiper les révolutions numériques qu'ont insufflées successivement la généralisation de l'internet, le *web* 2.0 et le grand dévoilement sur les réseaux sociaux, le *cloud* et le *big data*. 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 l'importance de pouvoir traiter les données allant de pair avec la nécessité d'une protection des individus en adéquation avec la réalité technologique advenue.

Ce règlement qui est en vigueur depuis le 25 mai 2016 et entrera en application le 25 mai 2018 doit être soigneusement pris en considération par les acteurs du terrain, tant du secteur privé que du secteur public, sur le sol européen comme sous des latitudes plus lointaines. En effet, une série d'adaptations, de nouveautés, voire de bouleversements ont été apportés en la matière dont le moindre n'est pas le changement du champ d'application territorial de la réglementation européenne qui, comme on le verra ci-dessous, a désormais vocation à régir les activités de nombreux acteurs situés au-delà des frontières de l'Union européenne.

Les pages qui suivent se focalisent sur les lignes de force du règlement et les principales nouveautés qu'il comporte[3].

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.

La voie ouverte à une inflation des règles en matière de protection des données. — Une singularité du règlement qui saute immédiatement aux yeux est sa longueur : 99 articles et pas moins de 173 considérants. Le texte, largement inspiré de celui de la directive, apporte des précisions là où des lacunes avaient suscité ou pourraient susciter des discussions ; il définit de nouveaux concepts et développe de nouvelles règles ; et il intègre des règles inspirées du travail de la Commission européenne et du Groupe de l'Article 29. Cet effort d'enrichissement n'est toutefois pas gage d'élimination de toute difficulté d'interprétation.

Par ailleurs, il est à noter que le 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.

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

(*) Cécile de Terwangne est professeur à la Faculté de droit de l'UNamur et directrice de recherche au CRIDS. Elle peut être contactée à l'adresse cecile.deterwangne@unamur.be. Karen Rosier est maître de conférences à la Faculté de droit de l'UNamur, chercheuse au CRIDS et avocate. Elle peut être contactée à l'adresse karen.rosier@unamur.be. Bénédicte Losdyck est chercheuse au CRIDS et avocate. Elle peut être contactée à l'adresse benedicte.losdyck@unamur.be. **(1)** 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). **(2)** Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. **(3)** Pour une analyse plus détaillée de ces nouveautés, voy. C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, pp. 5-57.

différents aspects de la protection des données[4]. Pour assurer la transition vers le nouveau régime, le Groupe de l'Article 29 a déjà initié le processus et publié des premières lignes directrices sur certains aspects du règlement[5].

Le règlement : un texte par et pour des spécialistes ? — L'inflation de règles et de directives plus précises 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. 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. 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 d'un délégué à la protection des données justifiant de connaissances spécialisées en la matière[6]). 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.

1 Champ d'application

A. Champ d'application matériel

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. L'exemption totale de l'application aux traitements effectués par une personne physique dans le cadre d'une activité strictement personnelle au domestique est maintenue (*cfr* article 2, § 2, c) du règlement).

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[7]. Une personne sera identifiable dès qu'elle pourra être traitée différemment de la masse, individualisée (la version anglaise utilise le terme *singling out*, soit l'individualisation ou le ciblage). 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 connaisse ou puisse connaître l'identité de la personne[8]. On opère un glissement de la notion d'identification vers un concept d'individualisation.

B. Champ d'application territorial

Changement de paradigme et déjà de nouvelles zones d'ombres. — 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. Le règlement fait sur ce point référence au lieu d'établissement du responsable du traitement ou du sous-traitant[9].

Reste une question de taille qui n'est pas — ou plutôt qui n'est plus — réglée par le règlement : les États membres conservent la possibilité de légiférer pour certains aspects ou types de traitements[10]. Le règlement ne définit pourtant pas quel sera le critère de rattachement dans ce cas[11]. 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.

(4) Voy. articles 68 et 70 du règlement. (5) 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. À ce jour quatre documents concernant respectivement les délégués à la protection des données, la portabilité, l'analyse d'impact et la détermination de l'autorité de contrôle compétente ont été adoptés et publiés sur le site http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083. (6) Articles 37 et suivants du règlement. (7) 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. (8) Considérant 26 du règlement. (9) Sur cette notion voy. article 4.16 du règlement. (10) Tout risque de disparité entre les législations nationales n'est donc pas éliminé. Le règlement maintient pour les États un pouvoir de prévoir des règles spécifiques pour des traitements qui poursuivent certaines finalités (dans le secteur public par exemple), qui portent sur certaines catégories de données (données sensibles et données « judiciaires »), qui concernent certaines catégories de personnes (les mineurs), ou encore 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 trouvé (l'équilibre à réaliser avec la liberté d'expression, notamment). (11) 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.

Analyse

La localisation de l'établissement du sous-traitant entrera en ligne de compte pour l'application territoriale du règlement. — Le règlement 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[12]. Les notions de « responsable du traitement » et de « sous-traitant » restent inchangées[13].

Il conviendra donc de vérifier comme par le passé si le traitement a lieu *dans le cadre des activités* d'un établissement localisé sur le territoire de l'Union, 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.

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 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[14], a soulevé des questions d'interprétation et de praticabilité. Il n'est plus repris dans le règlement mais l'application extraterritoriale revient par le biais de dispositions nouvelles.

De nouveaux critères liés à la localisation du public cible pour toucher les responsables du traitement établis hors de l'Union européenne. — 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[15]. Un parallèle peut être fait 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[16] et le règlement sur la compétence judiciaire[17]. 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 ultérieure 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.

(12) Article 3, § 1er, du règlement. **(13)** Articles 4, 7), et 4, 8), du règlement. **(14)** Voy. le document de travail du Groupe de l'Article 29 du 30 mai 2002 sur l'application internationale du droit de l'Union européenne en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites *web* établis en dehors de l'Union européenne (p. 12). **(15)** 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). **(16)** *Cfr* article 6 du règlement (CE) no 93/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I). **(17)** Article 17 du règlement (UE) no 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.

2 Redéfinition de certains aspects clés du traitement

A. Principes de licéité des traitements de données

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.

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 que la doctrine le rattachait jusqu'alors à l'exigence de loyauté[18]. Ce principe de transparence est explicité dans un long considérant[19] qui commence par préciser que le fait que des données sont collectées et utilisées 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[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, § 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 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[21].

Une autre nouveauté du règlement est la clarification du fait qu'il est permis dans deux cas de traiter des données à une fin différente de celle pour laquelle elles ont été collectées, sans s'interroger sur la compatibilité de cette nouvelle finalité avec la première : avec le consentement de la personne concernée pour ce traitement ultérieur ou lorsque celui-ci est fondé sur le droit de l'Union ou le droit national.

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[22]. 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 »[23].

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 »[24]. 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)[25]. 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[26].

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, § 1er, d), apportant cette précision que la rectification doit être faite « sans tarder ».

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

(18) Article 5, 1, a), du règlement. (19) Considérant 39 du règlement. (20) Voy. *infra*, p. 20. (21) Voy. Egalement considérant 50 du règlement. (22) Ces conditions sont développées à l'article 89, § 1er, du règlement. (23) Article 5, § 1, 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 ». (24) Considérant 30 de la proposition de règlement publiée le 25 janvier 2012 par la Commission européenne, COM(2012) 11 final. (25) 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 http://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 ». (26) Considérant 39 du règlement.

Analyse

Principe d'intégrité et 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[27] 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.

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[28].

B. Hypothèses de licéité des traitements de données

Hypothèses plutôt que conditions. — L'article 6, § 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. 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.

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 et considère qu'il « s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données »[29]. 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 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. On ne peut plus recourir au consentement implicite puisque seule une « manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »[30] est admise au titre de consentement. 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[31]. Dans ce cas, le responsable du traitement doit obtenir le consentement *explicite* de l'individu s'il choisit ce fondement pour légitimer son traitement[32].

Cela signifie-t-il la fin de la prédominance du consentement en tant que fondement ? 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. Premièrement, le consentement sera plus difficile à obtenir car les règles en la matière seront désormais plus strictes[33]. 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. La seconde raison pour laquelle il devrait moins être recouru au consentement 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[34]. La facilité avec laquelle l'individu va pouvoir retirer son consentement 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[35]. 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[36]. En conséquence, le responsable du traitement, lorsqu'il traite des données sur la base du consentement, est susceptible non seulement de se retrouver inopinément sans fondement légal pour traiter ces données, mais de devoir également les effacer.

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.

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, comme le traitement. Le considérant 46 offre un exemple de situation où le traitement de données est justifié par la sauvegarde d'intérêts vitaux : lorsqu'il est nécessaire à des fins humanitaires, par exemple pour suivre la propagation d'épidémies ou dans le cas de catastrophes naturelles.

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. — 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 son entrée en vigueur. Les États peuvent à l'avenir également introduire de telles dispositions sectorielles[37]. Les paragraphes 2 et 3 de l'article 6 apportent tou-

(27) Section 2 du chapitre IV consacré aux devoirs des responsable et sous-traitant, articles 32 à 34. Voy. *infra*, p. 18. (28) Voy. Egalement article 24 du règlement et *infra* p. 13. (29) 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 Jan Philipp Albrecht, 21 novembre 2013, exposé des motifs, pp. 218-219. (30) Article 4, 11), du règlement. (31) Article 9, § 1, du règlement. (32) Article 9, § 2, a), du règlement. (33) Les exigences supplémentaires sur ce point s'inspirent des recommandations émises dans l'avis n° 15/2011 par le Groupe de l'Article 29 sur la définition du consentement, 13 juillet 2011, WP 187. (34) Article 7, § 3, du règlement. (35) Article 7, § 3, du règlement. (36) Article 17, § 1, b), du règlement. (37) « 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 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

tefois 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. 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[38].

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 »[39] du responsable du traitement ou 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 »[40].

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[41]. 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 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[42] ou ceux visant à garantir la sécurité du réseau et des informations[43].

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[44]. 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[45].

C. Le traitement de données sensibles

Données sensibles par nature et selon le contexte. — Le règlement identifie, comme la convention 108 et la directive avant lui, des données qui sont, par nature, particulièrement sensibles du fait qu'elles mettent en jeu des libertés et droits fondamentaux. La liste des données sensibles figurant dans la directive a été reprise et quelque peu étoffée. Ainsi, à côté des données qui révèlent 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 les données génétiques et les données biométriques traitées aux fins d'identifier une personne physique de manière unique[46].

Le contexte dans lequel ces données sont traitées peut engendrer des risques pour les droits et libertés[47]. L'impact du contexte sur le caractère 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.

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[48].

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

une brèche importante dans l'acquis censé apporté par le règlement : l'unification des règles au niveau européen. » (T. Leonard et D. Chaumont, « GDPR.expert, Article 6 Licéité du traitement », 20 avril 2016, disponible sur http://www.gdpr-expert.eu/difficultes-probables.html?id=6). **(38)** C. 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. **(39)** 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 « nécessaire à la réalisation des intérêts légitimes (...) » à une formulation moins heureuse « nécessaire aux fins des intérêts légitimes (...) ». **(40)** Article 6, § 1er, f), du règlement. **(41)** Article 6, § 1, 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 Jan Philipp Albrecht, 17 décembre 2012). **(42)** Considérant 47. **(43)** Considérant 49. **(44)** Article 6, § 1er, alinéa 2, du règlement. **(45)** Considérant 47. **(46)** Article 9 du règlement. **(47)** Considérant 51. **(48)** Voy. les dix exceptions prévues à l'article 9, § 2, a) à j), du règlement.

Analyse

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 »[49].

Les données relatives aux condamnations pénales et aux infractions. — Une disposition spécifique[50] est consacrée au traitement des données relatives aux condamnations pénales et aux infractions ou mesures de sûreté connexes[51]. Ce qui est prévu est sommaire et très semblable à ce qui figurait dans la directive[52]. 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 toutefois désormais couverts par la directive 2016/680 du 27 avril 2016[53].

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[54]. 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

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 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 obtenir l'identité des 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.

3 Responsabilisation accrue des acteurs

A. Sous l'angle de la prévention des risques

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 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.

Le rôle du sous-traitant, entre exécutant et conseiller avisé. — Par ailleurs, de nouvelles obligations sont directement mises à charge du sous-traitant[55]. 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[56]. 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. 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[57].

1. Le principe de responsabilité (*accountability*)

Respecter la réglementation n'est plus suffisant : il va falloir pouvoir le démontrer. — Ce principe vient sanctionner les autres principes clés du traitement que nous avons évoqués ci-dessus.

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[58]. C'est ce que désigne le « principe de responsabilité » entendu non pas comme impliquant essentiellement une obligation de réparer le dommage en cas de violation de

(49) Article 9, § 2, g), du règlement. (50) Article 10 du règlement. (51) Ces données sont mentionnées dans la suite du présent texte sous l'appellation de « données judiciaires ». (52) Article 8, § 5, de la directive. (53) 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.* L 119/89 du 4 mai 2016. (54) Article 87 du règlement. (55) Article 28 du règlement. (56) Article 28, § 3, du règlement. (57) Article 28, § 3, h), alinéa 2, du règlement. (58) Article 5, § 2, du règlement.

la réglementation[59], 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[60]). Cela suppose donc une certaine proactivité et anticipation des critiques que l'on pourrait formuler à l'égard d'un traitement.

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 de mesures à prendre pour certains types de traitements ou responsables de traitement. 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 respecte les obligations qui lui incombent en vertu de l'article 28 du règlement[61].

2. Le registre des traitements

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.

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 les 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.

3. L'analyse d'impact

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, § 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 »[62].

Omniprésente dans le règlement, cette notion de « risque » n'est pas définie[63]. Dans une version intermédiaire de la proposition de règlement[64], 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 ».

Il s'agira d'apprécier le risque au cas par cas sur la base des quelques balises déjà identifiées dans le règlement et des lignes directrices consacrées à cette question publiées récemment par le Groupe de l'Article 29[65]. Le règlement 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[66]), (ii) le traitement à grande échelle de données sensibles[67] 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*.

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[68]. 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.

(59) Comparez avec l'article 23 de la directive intitulé « responsabilité ». **(60)** Voy. *infra*, p. 19. **(61)** Article 28, § 3, h), du règlement. **(62)** 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. **(63)** Voy. C. Burton, L. De Boel, C. 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, 1/25/2016, p. 7. **(64)** 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). **(65)** Groupe de l'Article 29, « Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 », WP 248, 4 avril 2017. **(66)** Considérant 91 du règlement. **(67)** Le Considérant 91 du règlement précisant 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*. **(68)** 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 — française — nationale Informatique et Libertés) relative aux analyses d'impact accessibles sur https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil.

Analyse

Consultation de l'autorité de contrôle. — Ces obligations se doublent d'une obligation pour le responsable du traitement de 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*[69]. 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. 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.

L'autorité de contrôle peut ainsi conseiller le responsable du traitement sur ce qu'il convient de faire[70] 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

Une nouvelle fonction pour qui et pour quoi ? — De spécialiste, il en sera 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[71]. 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[72]. Le délégué peut être un membre du personnel ou un tiers prestant dans le cadre d'un contrat de services[73]. 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[74]. Le règlement précise notamment que le délégué ne peut être pénalisé ou relevé de ses fonctions pour l'exercice de ses fonctions.

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[75]. 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[76]. 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[77]. 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[78].

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 publié des lignes directrices sur le sujet en vue de l'entrée en vigueur du règlement qui apporte des précisions sur les spécificités de la fonction[79].

5. Protection dès la conception et par défaut

Pour une protection paramètres 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 choix de moyens, y compris technologiques, qui permettent de respecter les principes en matière de protection des données.

(69) Article 36 du règlement. **(70)** Article 58, § 3, a), du règlement. **(71)** Article 37 du règlement. La notion n'est toutefois pas tout à fait neuve dès lors qu'elle existait déjà 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). **(72)** Article 37, § 5, du règlement. Pour les fonctions du délégué, voy. l'article 39, §1er, du règlement. **(73)** Article 37, § 6, du règlement. **(74)** Article 38, §§ 2 et 3, du règlement. **(75)** Article 37, §§ 1 et 4, du règlement. Se posera donc la question de la qualification de la fonction qui sera dévolue à un juriste chargé des aspects 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. **(76)** Article 37, § 1, a). **(77)** Article 37, § 1, a) et b), et considérant 97 du règlement. **(78)** Article 37, § 4, du règlement. **(79)** Groupe de l'Article 29, « Guidelines on Data Protection Officers ("DPOs") », WP 243, 13 décembre 2016, révisées et adoptées le 5 avril 2017.

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[80]. 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 énoncés à l'article 5 du règlement.

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 »[81].

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 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[82].

B. Sous l'angle de la gestion des risques

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

Faille dans la sécurité des données. — Les données doivent être traitées de façon à ce que leur sécurité soit garantie de manière appropriée, à l'aide des mesures techniques ou organisationnelles adéquates[83]. 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.

Obligation de notification. — Une fois le règlement applicable, tous les responsables de traitement auront une obligation légale de notifier les violations de données à caractère personnel dont ils sont victimes. Ces violations ne se limitent pas à la fuite accidentelle de données mais couvrent toute « 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 »[84]. Compte tenu de cette définition extensive, les notifications auprès de l'autorité de contrôle interviendront plus souvent qu'on aurait pu le penser.

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 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[85]. 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.

Notification à la personne concernée. — En outre, à moins que les données 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[86]. 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[87].

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[88]. 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.

2. Le nouveau régime de responsabilité

Régime prévu par la directive. — 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

(80) Article 25, § 1er, du règlement. (81) Article 25, § 2, du règlement. (82) Voy. le considérant 78 du règlement. (83) Article 5, § 1, f), du règlement ; voy. également E. Thole, « How to handle data breaches from EU legal and practical perspective », *in Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 231-233. (84) Article 4, 12), du règlement. (85) Article 33, § 5, du règlement. (86) Article 34, § 1, du règlement. (87) Article 34, § 3, c), du règlement. (88) Article 33, § 2, du règlement.

Analyse

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[89] : lorsqu'il n'a pas respecté les instructions licites données par le responsable du traitement et lorsqu'il n'a pas respecté les obligations que le 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[90]. 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.

Multiplication des recours. — Le règlement entend renforcer les voies de recours mises à disposition des personnes qui estiment que leurs droits 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[91]. Une telle procédure pourra déboucher sur l'imposition d'importantes amendes administratives par l'autorité de contrôle[92].

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[93].

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 a.s.b.l., 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[94]. Les États membres peuvent, s'ils le souhaitent, 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[95].

4 Renforcement de la protection des droits des personnes concernées

Maîtrise renforcée sur les données. — L'un des objectifs du nouveau 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 dispose désormais d'un véritable arsenal de droits dont l'exercice devrait se trouver facilité.

A. Consolidation des droits existants

Le règlement reprend l'ensemble des droits conférés par la directive mais va plus loin en renforçant certains d'entre eux.

Obligation de transparence accrue. — À partir du 25 mai 2018, chaque responsable du traitement devra fournir à la personne concernée, par écrit ou par d'autres moyens (par voie électronique par exemple), une série de nouvelles informations qu'il ne devait pas transmettre auparavant.[96]. 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 : des informations plus complètes sur le traitement[97] et des renseignements additionnels quant aux modalités d'exercice des droits[98].

Ces informations doivent être fournies de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant[99]. Si par le passé, le responsable du traitement devait déjà communiquer des 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 de remédier à ce problème en mettant l'accent sur la transparence et la clarté des informations. L'utilisation d'icônes[100] 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.

1. Droit d'opposition simplifié

Renversement de la charge de la preuve. — 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. La directive exigeait que la personne concernée désirant s'opposer au traitement de ses données démontre « des raisons prépondérantes et légi-

(89) Article 82, § 2, du règlement. (90) 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. (91) Article 77, § 1, du règlement. (92) À ce sujet voy. *infra*, p. 26. (93) Article 78 du règlement. (94) Article 80, § 1, du règlement. (95) Article 80, § 2, du règlement. (96) Article 12, § 1, du règlement. (97) Telles que par exemple, la base juridique du traitement, la source des données ou les intentions de transferts vers des pays tiers. (98) À titre d'exemples, le droit d'introduire une réclamation auprès de l'autorité de contrôle doit être indiqué, de même que les nouveaux droits à la portabilité des données et à la limitation du traitement etle droit de retirer son consentement à tout moment. (99) Article 12, § 1, du règlement. (100) Article 12, § 7, du règlement.

times 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 pour la personne concernée qui 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 de prouver que ses intérêts légitimes et impérieux prévalent sur les intérêts de la personne concernée[101]. Le règlement opère donc un renversement de la charge de la preuve au profit de la personne concernée.

Comme sous la directive, si le traitement est réalisé à des fins de prospection (marketing direct, par exemple), la personne concernée pourra s'y opposer sans justification aucune et aucune réplique n'est permise pour le responsable du traitement[102].

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[103].

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

Définition. — L'article 15 de la directive abordait déjà la problématique des décisions individuelles automatisées. Le règlement va plus loin et inclut le profilage entendu comme « 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 »[104]. Cette définition est très large et inclut notamment la publicité comportementale et la géolocalisation des individus.

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[105].

Exceptions. — Il y a toutefois trois situations dans lesquelles cette interdiction est levée[106] : lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne et le responsable du traitement ; lorsqu'elle est autorisée par une disposition légale prévoyant des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; lorsque la personne concernée a consenti 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 de vue ainsi que de contester la décision automatisée[107].

Les décisions individuelles automatisées admises ne peuvent toutefois pas être fondées sur des données sensibles, à moins que la personne ait donné son consentement explicite ou que ce soit nécessaire pour des motifs d'intérêt public important et que des mesures appropriées de sauvegarde soient prises[108].

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

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[109]. La Cour de justice a apporté, dans son désormais célèbre arrêt *Google Spain*[110], 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.

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 »[111].

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 consé-

(101) Considérant 69 du règlement. (102) Article 21, § 2, du règlement. (103) Article 21, § 4, du règlement. (104) Article 4, 4), du règlement. (105) Considérant 71 du règlement ; voy. également A. Grosjean, « Le profilage : un défi pour la protection des données à caractère personnel », *in Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 302. (106) Article 22, § 2, du règlement. (107) Article 22, § 3, du règlement. (108) Article 22, § 4, du règlement. (109) 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 Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 237-268. (110) C.J., 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja Gonzàlez*, aff. 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. (111) Considérant 65 du règlement.

Analyse

quences 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.

Le droit à l'effacement en aval. — « Afin de renforcer le "droit à l'oubli numérique" »[112], l'article 17, § 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 »[113].

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 95/46[114]. 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.

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'intérêt public, le traitement des données pourra se poursuivre.

3. Le droit à la limitation du traitement

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 12b 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[115] 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 »[116]. 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[117].

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

Nouvelles prérogatives. — L'article 20 du règlement reconnaît un véritable nouveau droit : le droit à la portabilité des données[118]. Celui-ci se subdivise en deux prérogatives. D'une part, les personnes concernées ont le droit de recevoir du responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, les données qu'elles lui ont fournies, et d'autre part, elles ont le droit de transmettre ces données à un autre responsable du traitement. Néanmoins, l'étendue du droit à la portabilité des données sera inévitablement 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 ».

Conditions cumulatives d'exercice. — L'exercice de ce droit est toutefois conditionné à la réunion simultanée de deux conditions. Premièrement, le traitement doit avoir été 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[119]. 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[120].

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. En effet, cela risque de constituer une barrière considérable à l'exercice effectif du droit à la portabilité des données[121].

Notion de « données fournies ». — Au surplus, seules les données fournies par la personne au responsable du traitement sont l'objet de ce droit. Le règlement ne donne aucune indication sur

(112) *Ibidem*. **(113)** *Ibidem*. **(114)** L'article 12, c), de la directive 95/46 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 ». **(115)** 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" ». **(116)** Article 4, 3), du règlement. **(117)** Article 18, § 1, du règlement et considérant 67 du règlement. **(118)** Voy. également Groupe de l'Article 29, *Guidelines on the right to data portability*, WP 242, 13 décembre 2016, révisées et adoptées le 5 avril 2017. **(119)** Article 20, § 1, a) et b), du règlement. **(120)** Article 20, § 2, du règlement. **(121)** Considérant 68 du règlement.

l'interprétation qu'il convient de faire des termes « données fournies ». Doit-on les limiter aux données procurées par l'individu ou peut-on leur reconnaître une portée plus large[122] ? 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 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. Etendre le droit à la portabilité 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. Il ne nous semble pas que ce nouveau droit à la portabilité doive recevoir une telle portée[123]. Il est à noter que le droit d'accès 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[124]. Ainsi, en vertu de ce droit, la personne aura accès à son profil de consommation établi par le responsable du traitement grâce au profilage par exemple.

Le droit à la portabilité des données renforce indéniablement l'emprise qu'ont les individus sur leurs données. Destiné à favoriser la mobilité des clients dans l'environnement en ligne, il pose indéniablement des questions en matière de propriété intellectuelle et de droit de la concurrence.

5 Flux transfrontières de données

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'Union européenne 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[125], ou enfin qu'une dérogation trouve à s'appliquer[126].

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[127].

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

6 Accentuation du rôle des autorités de contrôle et renforcement des sanctions

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, et des mécanismes de coordination et de répartition des actions et compétences des différentes autorités nationales.

De manière générale, les autorités de contrôle voient leurs pouvoirs en matière de guidance dans l'application de la réglementation[128] et de mesures « correctrices » en cas de mauvaise application de celle-ci élargis.

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 EUR ou, pour une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent[129]. Ceci devrait donner à réfléchir lorsqu'il sera question du degré de priorité à donner aux aspects « protection des données » d'un projet.

(122) Voy. notamment sur le sujet P. Valcke et J. Verschakelen, « Dataportabiliteit en digitale (mensen-)handel », *NjW.*, 9 avril 2014, pp. 298-300. (123) En ce sens, voy. Groupe de l'Article 29, *Guidelines on the right to data portability*, WP 242, 13 décembre 2016, p. 8. (124) Article 15, § 3, du règlement. (125) Ces règles sont couramment évoquées sous leur appellation anglaise : *binding corporate rules* (BCR). Elles sont définies à l'article 4, 20°, du règlement. (126) Articles 44 et s. du règlement. (127) 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, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_FR.pdf ; également C. Gayrel et R. Robert, « Proposition de règlement sur la protection des données - Premiers commentaires », *J.D.E.*, 2012, p. 179. Voy. la définition adoptée par le Contrôleur européen dans son document d'orientation « 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 », 14 juillet 2014, p. 7, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_FR.pdf. (128) Voy. l'article 57 du règlement. (129) Article 83 du règlement.

Analyse

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, en tenant compte de l'ampleur des traitements rendus possibles par la technologie et de leur caractère plus globalisé à l'échelle internationale.

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 qui se veulent plus dissuasives. 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, les avis du Comité européen et les *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 des 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.