Règlement général sur la protection des données : entre constance et innovation

« Il est parfois nécessaire de changer certaines lois mais le cas est rare, et lorsqu'il arrive, il ne faut y toucher que d'une main tremblante. »
Monstesquieu, *Lettres persanes*, Lettre CXXIX « Usbek à Rhédi, à Venise », 1721.

Le règlement européen renforce les droits et obligations introduits par la directive de 1995, mais reconnaît également de nouveaux droits aux personnes issus de l'évolution des technologies : portabilité des données, droit à l'oubli et droit de limitation. Enfin, il innove en passant d'un modèle de contrôle *a priori*, sur la base de formalités préalables, à un modèle d'autocontrôle, l'*accountability*.

XAVIER LEMARTELEUR

Responsable juridique technologies de l'information

Groupe La Poste

L'adoption du règlement européen sur la protection des données[1] s'inscrit dans le contexte des évolutions technologiques qui ont marqué les deux dernières décennies[2]. La vocation première de ce nouveau texte est donc de réaliser une « mise à jour » du cadre légal applicable à la protection des données face aux innovations technologiques, mais aussi de le réformer plus profondément, afin de prendre en compte les enseignements issus de vingt années de pratique de la protection des données en Europe.

Ce contexte et cette filiation expliquent sans doute le caractère dual de la nouvelle réglementation, à la fois marquée par d'importantes nouveautés (II.) et par une certaine continuité avec le cadre légal préexistant (I.).

I. LA RÉAFFIRMATION DES GRANDS PRINCIPES ISSUS DE LA DIRECTIVE DE 1995

Le règlement reprend, souvent en les renforçant, les droits et obligations qu'avait introduits la directive de 1995[3], il en va ainsi des droits reconnus aux personnes (1.) et des obligations mises à la charge du responsable de traitement (2.).

1. Réaffirmation des droits reconnus aux personnes

Le texte réaffirme, parfois en les ajustant à la marge, les grands droits reconnus aux personnes dont les données sont traitées. Il s'agit principalement des droits d'accès, d'opposition et de rectification.

Le droit d'accès[4] voit son étendue légèrement accrue. Les personnes pourront donc désormais, au titre de leur droit d'accès, avoir connaissance notamment de la durée de conservation[5] de leurs données mais aussi, et pour faire écho aux nouvelles dispositions sur le profilage[6], de « *l'existence d'une prise de décision automatisée, y compris un profilage, [...] au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée* ». L'apport reste donc limité.

Le doit d'opposition[7] ne connaît pas non plus de grand bouleversement, on notera simplement que son exercice est facilité. En effet, alors que

1. Règlement 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) ; n° 2016/679 du 27 avril 2016, JOUE n° L. 119, 4 mai 2016, p. 1.
2. Depuis l'adoption du cadre européen en matière de protection des données en 1995.
3. 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, qui elle-même s'inspirait de certaines législations nationales des États Membres et de la convention 108 (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe du 28 janvier 1981). Voir, dans ce même numéro, la synthèse d'Emmanuel Jouffin, p. 4. Nous entrerons dans les détails de quelques dispositions clés évoquées dans ladite synthèse.
4. Art. 15 du règlement.
5. Sur ce sujet : art. 32-I-8° de la loi Informatique et Libertés issu de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Les personnes concernées doivent avoir connaissance de « *la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée* ». Cf. art. 13-2 a et 14-2 a du RGPD qui évoquent la durée de conservation des données et non les « *catégories* » de données.
6. Sur ce point, voir, dans ce même numéro, la contribution d'Eric Caprioli., p. 23.
7. Art. 21 du règlement.

sous l'empire de la directive de 95[8] la personne devait justifier de « *raisons prépondérantes et légitimes tenant à sa situation particulière* » pour exercer son droit, elle n'aura désormais qu'à invoquer des « *raisons tenant à sa situation particulière* », à charge pour le responsable de traitement souhaitant ne pas faire droit à la demande de prouver « *qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée* ». Il s'agit là donc d'un renversement de la charge de la preuve dans le cadre de l'exercice du droit d'opposition.

Par ailleurs, ce droit comprend toujours la possibilité pour les personnes de s'opposer, sans qu'aucune justification n'ait à être apportée, au traitement ayant pour finalité la prospection commerciale.

Enfin on notera que le droit de suppression, à l'image de ce qui a été vu en matière de droit d'accès, fait référence à la possibilité de s'opposer au profilage, notamment en matière de prospection commerciale[9].

S'agissant du droit de suppression aucune modification particulière n'est à relever.

Les modalités d'exercice de ces différents droits sont encadrées par un nouvel article[10], absent de la directive de 95. Celui-ci impose que le responsable de traitement transmette des informations à la personne concernée « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* ». Cette nouvelle obligation, qui trouve également à s'appliquer en matière d'information des personnes, prend tout son sens dans le contexte de l'exercice du droit d'accès. Il appartiendra alors au responsable de traitement de s'assurer que les données communiquées au demandeur sont claires et aisément compréhensibles. L'exercice pratique peut s'avérer particulièrement complexe lorsque le volume de données est important, dans ce cas il pourrait être nécessaire d'en faire une synthèse aisément appréhensible[11].

Ce même article encadre également les délais dans lesquels il devra être fait droit aux demandes. Le responsable de traitement devra ainsi répondre « *dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande* »[12].

2. Réaffirmation des obligations du responsable de traitement

Le responsable de traitement doit, comme par le passé, informer les personnes du traitement qu'il met en œuvre. Cette obligation d'information est cependant assez largement renforcée par le règlement qui consacre deux articles distincts selon qu'il s'agisse d'une collecte directe de données[13] ou d'une collecte indirecte[14].

Dans le cas d'une collecte directe, au travers d'un bulletin de souscription par exemple, les mentions suivantes devront être portées à la connaissance de la personne :
– identité et coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;
– le cas échéant, les coordonnées du délégué à la protection des données ;
– les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;
– les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers s'ils constituent le fondement du traitement[15] ;
– les destinataires ou les catégories de destinataires des données à caractère personnel ;
– le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers et les garanties encadrant ce transfert ainsi que les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

Le responsable de traitement doit également communiquer les informations suivantes :
– la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
– l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
– lorsque le traitement est fondé sur le consentement, l'existence du droit de retirer son consentement à tout moment ;
– le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
– des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
– l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Dans le cas d'une collecte indirecte s'ajoute à cette longue liste : la source des données (c'est-à-dire l'identité du responsable de traitement qui a transmis les données) et les catégories de données concernées (c'est-à-dire les typologies de données qui ont été transmises)[16].

On assiste donc à une inflation importante des informations devant être communiquées aux individus,

8. Art. 14 de la directive.
9. Il est vrai que le profilage en matière commerciale est devenu particulièrement intrusif, notamment lorsqu'il est réalisé par le biais du suivi de la navigation sur internet (via les *cookies*). À ce titre le futur règlement ayant vocation à remplacer la directive 2002/58, dite directive *e-privacy*, dont une première proposition a récemment été présentée, devrait largement limiter les facultés de profilage lors de la navigation sur l'internet.
10. Art. 12 du règlement.
11. Sur cet aspect, voir *infra* : développement concernant le droit à la portabilité des données.
12. Le délai peut toutefois être prolongé de 2 mois « *compte tenu de la complexité et du nombre de demandes* ». Dans ce cas le responsable de traitement doit en informer la personne concernée.
13. Art. 13 du règlement.
14. Art. 14 du règlement.
15. Si le traitement est fondé sur l'article 6, paragraphe 1, point f).
16. Il s'agit là d'un apport important du règlement dans la mesure où il permettra aux personnes de disposer d'une certaine traçabilité sur leurs données. Elles pourront ainsi exercer leurs droits directement auprès du responsable de traitement à l'origine de la transmission des données. Cela est d'autant plus utile dans le secteur du *marketing* direct dans lequel les cessions de données sont particulièrement courantes.

alors que, dans le même temps, l'article 12 du règlement, impose au responsable de traitement une obligation de transparence[17]. Il conviendra donc de faire œuvre de pédagogie afin de s'assurer que l'information reste claire, simple et concise… voilà qui risque de relever de la gageure… Rappelons que, compte tenu des limites propres au moyen de communication utilisé, est une pratique commerciale trompeuse le fait d'omettre, dissimuler, fournir de façon inintelligible une information substantielle (art. L. 121-3, al. 1er, du Code de la consommation)[18].

Au titre des obligations à la charge du responsable de traitement « réaffirmées », on citera, sans s'y appesantir, l'obligation d'assurer la sécurité des données traitées[19], ainsi que les autres grands principes sur lesquels s'appuie la protection des données personnelles tels que : la fixation d'une durée de conservation des données au regard de la finalité du traitement, le principe de loyauté, de finalité et de proportionnalité[20].

Par ailleurs, le texte réaffirme la nécessité de principe[21] de recueil du consentement des personnes au traitement de leurs données.

La réaffirmation de ces droits et obligations par le règlement, même s'ils sont souvent adaptés et renforcés, montre une continuité avec la directive de 1995 et les grands principes qui ont marqué la protection des données à caractère personnel en Europe depuis sa genèse. Toutefois, le texte ne se contente pas simplement de reprendre des concepts anciens, il innove aussi assez largement en introduisant de nouveaux droits au profit des personnes et de nouvelles obligations à la charge des responsables de traitement.

II. LES INNOVATIONS DU RÈGLEMENT EUROPÉEN

Le texte marque une certaine rupture avec les concepts anciens, en reconnaissant de nouveaux droits aux personnes trouvant leur justification dans l'évolution des technologies(1.). Mais là où le règlement innove réellement c'est dans l'appréhension des modalités de mise en conformité à la réglementation, passant d'un modèle de contrôle *a priori* sur la base de formalités préalables, à un modèle d'autocontrôle (*accountability*) (2.).

1. La reconnaissance de nouveaux droits par le règlement

L'adoption du règlement a été l'occasion de reconnaître de nouveaux droits aux personnes dont les données sont traitées. Ces droits trouvent en grande partie, là encore, leur justification dans le développement de l'internet et plus particulièrement des réseaux sociaux. C'est ainsi que le droit à la portabilité des données, le droit à l'oubli ou encore le droit de limitation font leur apparition.

1.1. Portabilité des données

L'article 20 du texte permet aux personnes de « *recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement* ». Il s'agit d'une réversibilité légale reconnue au profit des individus ayant pour objet de leur permettre de changer de plateforme tout en conservant l'historique de leurs données. Dans le cas d'un réseau social, par exemple, cette disposition permettrait ainsi de basculer l'intégralité d'un profil vers une autre plate-forme de réseau social. L'esprit du texte est louable même s'il ne va pas sans quelques difficultés d'application aux entreprises plus « traditionnelles ».

En préalable, il est important de noter que ce nouveau droit n'est pas absolu. Il n'est en effet ouvert que dans certaines situations limitées à savoir : lorsque le traitement est fondé sur le consentement de la personne[22] ou encore sur la base de l'exécution d'un contrat[23] et que le traitement est réalisé à l'aide de procédés automatisés[24].

L'étendue du droit à la portabilité des données ainsi que ses modalités de mise en œuvre restent encore confuses. Afin d'en préciser le contour, le Groupe de l'article 29[25] a récemment publié des lignes directrices ayant vocation à détailler le contenu de ce nouveau droit[26].

L'interrogation porte notamment sur l'étendue des données soumises au droit à la portabilité. À ce titre, les lignes directrices du G29 tracent une limite entre les informations directement transmises par la personne concernée et celles observées[27] de son activité qui entrent dans le champ la portabilité d'une part, et les données déduites ou dérivées[28] qui n'y sont pas

17. Cf. *supra* les développements concernant le droit d'accès.
18. Ces pratiques donnent lieu à une sanction pénale (art. L. 132-2 du Code de la consommation) : emprisonnement de deux ans et amende de 300 000 euros. Le montant de l'amende peut être porté, de manière proportionnée aux avantages tirés du délit, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits, ou à 50 % des dépenses engagées pour la réalisation de la publicité ou de la pratique constituant ce délit.
19. On notera cependant que l'article 32 du règlement se veut plus détaillé que ne l'était la directive. Il fait ainsi directement référence à l'utilisation de procédés de chiffrement ou de pseudonymisation ainsi qu'aux piliers qui fondent la sécurité des systèmes d'information que sont la confidentialité, intégrité, disponibilité et résilience. Voir, dans ce même numéro, la contribution de Christophe Boutonnet, p. 52.
20. Ces grands principes sont rappelés à l'article 5 du règlement. Concernant la « proportionnalité », le règlement va plus loin que la directive de 95 en prévoyant que les données doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)* ». On voit reconnaître ici, un peu timidement, le principe de minimisation qui avait été proposé à l'origine par la Commission européenne. Selon ce principe, seules les données strictement nécessaires au traitement peuvent être collectées et traitées, alors que la directive de 95 prévoit pour sa part que les données ne doivent pas être excessives au regard de la finalité.
21. En effet, le principe de recueil du consentement au traitement des données prévu par l'article 6 du règlement connaît un nombre important d'exception, faisant *in fine* tomber le principe dans l'exception. On notera qu'il en était de même en vertu de l'article 7 de la directive 95/46.
22. Cela renvoie aux conditions de licéité du traitement prévues par l'article 6 du règlement et plus particulièrement au point 1.a.
23. Art. 6 1.b du règlement.
24. Il ne concerne dont pas les traitements manuels (papier).
25. Instauré par l'article 29 de la directive du 24 octobre, il s'agit d'un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales.
26. G29, *Guidelines on the right to data portability*, 16/EN WP 242, Adopted on 13 December 2016.
27. *Op. cit.*, page 8. Les lignes directrices distinguent les « *data actively and knowingly provided by the data subject* » telles que les informations communiquées au travers d'un formulaire de souscription ; les « *observed data* » qui sont des données qui découlent de l'utilisation du service par les utilisateurs (par exemple une liste de lecture sur un service de streaming de music ou encore les données issues du capteur d'un objet connecté) ; ces deux typologies de données étant susceptible de portabilité.
28. *Op. cit.*, page 8. Le texte original en anglais évoque les « *inferred data and derived data* ». Il s'agit en fait de données issues d'un traitement autonome mis

sujettes d'autre part. Si la distinction a le mérite de clarifier quelque peu le périmètre de l'obligation, il n'en demeure pas moins que, dans la pratique, les entreprises devront se livrer à une analyse casuistique qui risque de s'avérer complexe et laborieuse.

D'autant plus qu'aucune limite n'est prévue quant au volume de données transmises ou à l'utilité de ces données pour la personne concernée[29]. Bien au contraire, les lignes directrices prévoient, dans le cas où le volume de données est important, que le responsable de traitement fasse en sorte de les présenter sous forme de tableau de bord afin que la personne soit en mesure de comprendre la structure de ses données[30]. Il ne s'agit pas ici d'une simple recommandation du G29 mais de conditions à mettre en œuvre afin de respecter l'obligation générale de transparence dans l'exercice des droits instaurée par le règlement[31].

Les craintes que suscite cette portabilité sont nombreuses. Craintes sécuritaires tout d'abord, la prise en considération d'un niveau de sécurité comparable n'entrant pas en ligne de compte, craintes économiques liés à des transferts massifs de données[32], mais également au fait le G 29[33] estime que les droits de propriété intellectuelle, « *doivent être pris en considération avant de répondre à une demande de portabilité des données* », il estime néanmoins que « *le résultat de ces considérations ne devrait pas être un refus de fournir toutes les informations à la personne concernée* ». Cette affirmation laisse pensive alors même que les données objets de la portabilité peuvent être issues de base de données. La portabilité prend une coloration particulière dans le contexte de la Directive service de paiement II, laquelle ouvre le marché des paiements à de nouveaux acteurs, potentiellement directement bénéficiaires de ce nouveau droit.

In fine, il convient de noter que cette obligation a été introduite en droit national par anticipation par la loi République numérique[34]. Le texte, par un curieux ajout au Code de la consommation, étend même le principe en distinguant la portabilité des données selon qu'il s'agit ou non de données à caractère personnel. Dans le premier cas le cadre légal applicable est celui prévu par l'article 20 du règlement européen sur la protection des données, alors que dans le second cas, un régime *ad hoc* a été introduit dans le Code de la consommation. On notera à cet égard que la loi Lemaire évoque, au titre des exceptions à cette portabilité, les données « *ayant fait l'objet d'un enrichissement significatif par le fournisseur* », précision absente du réglement.

1.2. Droit à l'oubli

Présenté comme une des innovations majeures du règlement, le droit à l'oubli se voit expressément consacré[35] par le règlement. Sous l'empire de la directive de 95, et en France de la loi de 1978, ce droit connaissait déjà une existence[36] au travers de la faculté reconnue aux personnes de demander à ce que leurs données soient supprimées[37].

C'est d'ailleurs sur le fondement de la directive de 95 que la jurisprudence européenne a en premier lieu affirmé l'existence du droit à l'oubli numérique[38]. Il ne s'agit donc pas là d'une révolution mais d'un simple apport du règlement.

Quoi qu'il en soit, le droit à l'oubli, n'est pas un absolu. Son ouverture reste encadrée par certaines conditions d'exercice. Ainsi, il ne trouvera à s'appliquer que si l'une des conditions suivantes est réunie :

– les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
– la personne concernée retire le consentement sur lequel est fondé le traitement, [...], et il n'existe pas d'autre fondement juridique au traitement ;
– la personne concernée s'oppose au traitement[39] ;
– les données à caractère personnel ont fait l'objet d'un traitement illicite ;
– les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
– les données à caractère personnel ont été collectées auprès d'un enfant[40].

On constate qu'en réalité, l'innovation annoncée n'est que la conséquence naturelle de l'application des principes généraux en matière de protection des données : si les données n'ont plus de fondement à être traitées ; elles doivent être supprimées par le responsable de traitement. Le seul cas dans lequel cette nouvelle disposition constitue une avancée concerne les données communiquées par un mineur.

L'apport principal du droit à l'oubli nouvellement consacré repose sur les conséquences de son exercice. Il est en effet prévu par le texte[41] que le responsable de traitement doit informer les autres responsables de traitement (et sous-traitants) de la demande d'effa-

en place par le responsable de traitement, on pense notamment au traitement algorithmique. Dans ce sens, les lignes directrices citent à titre d'exemple le score attribué dans le cadre d'une demande de crédit (*credit scoring*).

29. On notera ainsi que les lignes directrices étendent largement sans aucune limite les données sujettes à l'obligation de portabilité. *In fine*, même en se limitant aux données directement transmises par la personne et à celles résultant de son utilisation directe d'un service, le volume de données peut être conséquent et s'étendre à des informations ne présentant que peu, voir aucun intérêt pour la personne. On peut penser notamment, dans le cadre d'un portail web bancaire, à l'historique des connexions d'un client.

30. *Op. cit.*, page 14, « how to deal with large and complex personal data collection ? ».

31. Article 12 du règlement précité.

32. *Op. cit.*, page 15. Le G29 évoque la création d'API (interface de programmation).

33. *Ibid.*, p. 10.

34. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, article 48.

35. Art. 17 du règlement.

36. Il est vrai que si la notion de « *droit à l'oubli* » connaît une existence de fait sous l'empire de la loi de 78, le texte ne contient aucune référence expresse à ce droit. Son affirmation repose sur l'obligation de ne pas conserver les données au-delà de la durée nécessaire à l'accomplissement de la finalité du traitement en vertu de l'art. 6 5°) de la loi 78-17 disposant que les données à caractère personnel « *sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ».

37. Art. 12 b) de la directive de 95 et art. 40 de la loi de 1978.

38. Arrêt de la Cour (grande chambre) du 13 mai 2014. *Google Spain SL et Google Inc. c/ Agencia Española de Protección de Datos (AEPD) et Mario Costeja González.* Demande de décision préjudicielle: Audiencia Nacional - Espagne. Affaire C-131/12.

39. Dans les conditions prévues par l'article 21 du règlement.

40. Tel que visé par l'article 8-1 du règlement.

41. Art. 17. 2. : « *Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.* »

cement afin que ceux-ci suppriment toute copie ou lien vers les données objet du droit à l'effacement. Il s'agit donc là d'une mesure particulièrement adaptée au contexte de l'internet dans lequel la réplication des informations entraîne une perte de contrôle par les personnes sur leurs données.

Mais là encore ce droit connaît une série de limites. Le droit à l'oubli doit ainsi céder face :
– au droit à la liberté d'expression et d'information ;
– à une obligation légale auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
– à des motifs d'intérêt public dans le domaine de la santé publique ;
– à la conservation à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
– à la constatation, à l'exercice ou à la défense de droits en justice.

1.3. Droit à limitation

Dernier droit nouvellement introduit[42] par le règlement, le droit à limitation permet aux personnes dont les données sont traitées d'imposer au responsable de traitement la conservation des données tout en en interdisant l'utilisation.

En pratique, le droit à limitation permet de suspendre le traitement des données lorsque :
– il existe un désaccord entre le responsable du traitement et la personne concernant l'exactitude des données[43] ou le fondement de l'exercice du droit d'opposition[44] ;
– les données sont traitées de manière illicite par le responsable de traitement, le droit à limitation intervient alors comme une mesure précontentieuse permettant à l'individu de demander la conservation de la preuve des manquements[45] ;
– enfin, il permet, dans le cadre d'un contentieux contre un tiers, de demander à un responsable de traitement la conservation des données qui pourront servir de preuve contre ce tiers[46].

L'ensemble des nouveaux droits reconnus aux individus vont avoir un impact en termes organisationnels pour les entreprises traitant des données à caractère personnel. Il conviendra ainsi de s'assurer, notamment au plan technique, que les systèmes d'information permettent de prendre en compte et de respecter ces nouveaux droits.

Si ces « innovations » ne sont pas neutres pour les entreprises et vont impliquer de nécessaires adaptations de leurs traitements, la réelle rupture introduite par le règlement concerne les obligations mises à leur charge, principalement au travers d'une vision nouvelle de la conformité : l'*accountability*.

2. De nouvelles obligations à la charge du responsable de traitement

Le règlement met à la charge des responsables de traitement tout un ensemble de nouvelles obligations (2.1.). Cependant la principale nouveauté provient de l'allégement des formalités préalables en matière de protection des données que sont les déclarations et demandes d'autorisation auprès de l'autorité de contrôle nationale. Cet assouplissement n'est cependant qu'apparent. Il se voit remplacé par un nouveau concept, l'*accountability* qui comporte d'importantes conséquences pour l'entreprise (2.2.).

2.1. Pot-pourri de nouvelles obligations

Il est délicat d'établir une liste totalement exhaustive des nouvelles obligations que les responsables de traitement devront respecter tant l'importance et la nature de ces obligations sont hétéroclites. On retiendra toutefois que les entreprises voient se renforcer leurs obligations en termes de sécurité au travers de l'établissement d'une notification des incidents ; il est également fait une place particulière au rôle du sous-traitant, imposant au responsable de traitement de s'assurer du sérieux de ses cocontractants.

Notification des incidents de sécurité

Une fois de plus cette innovation n'est pas apparue *ex nihilo* mais s'inscrit dans un cheminement dont les prémices remontent à près de quinze années[47]. Une application sectorielle avait ensuite été instaurée par la réglementation européenne[48]. C'est d'ailleurs cette obligation sectorielle que le règlement étend à l'ensemble des acteurs traitant de données à caractère personnel.

Ainsi, l'article 33 du règlement prévoit qu' « *en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente [...], dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* ».

Si l'autorité de protection considère que les mesures adéquates n'ont pas été prises pour protéger les données, alors il appartiendra au responsable de traitement d'informer individuellement les personnes dont les informations ont été compromises[49].

La vocation première de cette obligation, au-delà de permettre aux individus d'être avertis des risques d'usurpation d'identité dont ils pourraient faire l'objet, est d'inciter les responsables de traitement à investir dans la sécurité de leurs systèmes d'information et de s'assurer que leurs processus opérationnels prennent bien en compte l'impératif de sécurité. En effet, au-delà du risque d'image induit

42. Là encore il ne s'agit pas d'une réelle innovation mais de l'extension d'une faculté préexistante reconnue aux personnes. L'article 12 de la directive de 95 ainsi que l'article 40 de loi de 1978 établissaient déjà un droit de demander le « *verrouillage* » des données.
43. Art. 18 1. a) du règlement. Lorsque le responsable de traitement souhaite analyser l'équilibre entre l'intérêt légitime de la personne à ce que ses données ne soient pas traitées et son propre intérêt légitime à traiter les données.
44. Art. 18. 1. d) du règlement.
45. Art. 18. 1. b) du règlement.
46. Art. 18. 1. c) du règlement. Il convient de noter que cette faculté semble s'écarter assez largement des enjeux en matière de protection des données personnelles ; le droit ainsi reconnu transforme ainsi le responsable de traitement en séquestre de données dans un contentieux qui lui est pourtant étranger. Cela est d'autant plus discutable que le responsable, en vertu de l'article 12. 5. du règlement ne pourra répercuter les coûts induits par le droit de limitation.
47. La notification des incidents de sécurité est initialement apparue dans l'état de Californie en 2003. Elle a ensuite été assez largement adoptée par les différents États nord-américains, puis étendue au niveau fédéral notamment en matière de données bancaires (*Gramm Leach Bliley act*) et dans le secteur des assurances (*Health Insurance Portability and Accountability Act*- HIPAA).
48. Dans le secteur des télécommunications, cette obligation existe déjà depuis la refonte de la directive *e-privacy* (2002/58/CE) par la directive 2009/136/CE.
49. Art 34 du règlement.

par la publication dans la presse d'une perte de données, les coûts généralement associés à cette perte sont considérables [50].

Recours à la sous-traitance

Le règlement accorde une place nouvelle au sous-traitant. Alors que sous l'empire de la directive (et incidemment de la loi de 1978), ce dernier restait totalement dans l'ombre du responsable de traitement, il se voit désormais reconnaître un certain rôle, et donc une part de responsabilité dans le traitement de données par le règlement [51].

Si par le passé, le responsable devait recourir à des sous-traitants présentant des « garanties suffisantes » uniquement au regard de la sécurité des données [52], désormais plus généralement, ces « garanties suffisantes » concernent le respect de la réglementation sur la protection des données dans son intégralité [53].

Les conditions de recours à la sous-traitance sont par ailleurs plus précisément encadrées. Il est fait obligation au responsable de traitement de fixer contractuellement certaines exigences liées à la protection des données. Le contrat doit ainsi comporter les engagements suivants de la part du sous-traitant :

– qu'il « *ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers* […] » ;

– qu'il « *veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité* » ;

– qu'il assure la sécurité des données ;

– qu'il recueille le consentement du responsable de traitement dans le cas où il a lui-même recours à un sous-traitant. Dans ce cas qu'il s'assure que le contrat l'unissant à son propre sous-traitant comporte les mêmes obligations que celles qui lui ont été imputées ;

– qu'il « *aide le responsable du traitement, […] à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits* ». De même il doit assister le responsable de traitement dans le cadre de ses obligations en matière de sécurité de l'information et de notification des incidents de sécurité ;

– à l'issue du contrat, qu'il « *supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement* » ;

– qu'il mette à disposition du responsable du traitement « *toutes les informations nécessaires pour apporter la preuve du respect des obligations […] et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits* ».

De telles obligations devront donc conduire les entreprises à amender les contrats existants avec leurs sous-traitants et à intégrer dans les phases d'appel d'offres des critères permettant de s'assurer que le prestataire retenu répond aux nouvelles exigences du règlement [54].

Enfin, dans le monde bancaire et financier, la question de la soumission de ce type de contrats aux sujétions de l'arrêté du 3 novembre 2014 relatif au contrôle interne des banques devra, plus que jamais, se poser.

2.2. *Accountability*

Le passage d'une conformité fondée sur la réalisation de formalités préalables à un mécanisme d'autocontrôle et de prise en charge ab initio de la protection des données par l'entreprise constitue certainement la plus grande rupture introduite par le règlement [55].

Cette nouvelle appréhension du respect de la protection des données, dénommée « *accountability* », vise à mettre à la charge de l'entreprise la vérification de la conformité de ses traitements. Il lui appartiendra ainsi au regard « *de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes* » d'adopter « *des mesures techniques et organisationnelles appropriées pour s'assurer […] que le traitement est effectué conformément au […] règlement* » [56]. Elle doit par ailleurs d'être en mesure de démontrer à l'autorité de contrôle que les traitements qu'elle met en œuvre sont conformes à la réglementation. Notons que cette obligation concerne également les sous-traitants.

L'entreprise devient donc le premier garant de la protection des données. Elle devra « *lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement* » [57].

Une telle démarche comporte de nombreuses implications pour le responsable de traitement, notamment au plan organisationnel. Ce dernier devra ainsi modifier ses processus de gestion de projet afin d'y insérer des points de contrôle de la conformité à la protection des données et s'assurer que les différentes étapes ont bien été documentées.

L'*accountability* repose en effet sur une auto-évaluation par l'entreprise des traitements qu'elle met en place et la création d'une documentation constituant une sorte de piste d'audit que le régulateur pourra consulter. Cette documentation passe principalement par le maintien d'un registre des traitements [58] contenant :

– nom et coordonnées du responsable de traitement ;

– finalités ;

– catégories de personnes concernées et catégories de données à caractère personnel traitées ;

– destinataires ;

– transferts de données vers l'étranger.

Au-delà de la tenue d'une documentation, l'*accountabilty* implique de la

50. En ce sens, voir la dernière étude du Ponemon Institute « *2016 Ponemon Cost of Data Breach Study* ». Rapporté au monde entier, le coût est de 158 dollars par donnée perdue.

51. Art. 79 du règlement.

52. Art. 17 de la directive de 95 et 35 de la loi de 78.

53. Art. 28.1 du règlement.

54. À ce titre, il convient de noter que le règlement prévoit que l'adhésion à un code de conduite (art. 40) ou une certification (art.42) peut permettre de considérer que le prestataire apporte des garanties suffisantes au regard de la réglementation sur la protection des données.

55. Même si ce concept d'origine anglo-saxonne n'est cependant totalement nouveau dans le domaine de la protection des données, on le retrouve notamment, dès 1980, dans les OECD *Privacy guidelines* (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* du 23 septembre 1980 modifiée en 2013). Voir également Opinion 3/2010 *on the principle of accountability*, WP 173 du 13 juillet 2010.

56. Art. 24 du règlement.

57. *Ibid.*

58. Art. 30 du règlement. Il ne s'agira pas d'une grande nouveauté pour les entreprises qui avaient désigné un CIL, la tenue du registre des traitements étant une des missions lui étant confiées (article 22 de la loi Informatique et Libertés - article 47 du décret de 2005).

part de l'entreprise une approche différente des traitements qu'elle met en œuvre, celle-ci devant peser les risques induits par son projet pour la vie privée des individus.

Lorsque le traitement présente d'importants risques ou pour certains types de traitements prédéterminés[59], l'entreprise devra conduire une étude d'impact sur la vie privée (EIVP). La particularité de cette étude d'impact est de prendre pour point central non pas l'intérêt de l'entreprise mais le risque pour les personnes dont les données sont traitées. En synthèse, l'entreprise doit apprécier en quoi son traitement est « dangereux » pour les individus.

Cette analyse d'impact est formalisée dans un document devant comprendre *a minima* :
– la description des opérations de traitement ainsi que les finalités poursuivies ;
– une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
– une évaluation des risques pour les droits et libertés des personnes concernées ;
– les mesures envisagées pour faire face aux risques.

Il est certain que les modalités pratiques pour la conduite de ces études nécessiteront d'être précisées. À ce titre, on peut noter que la CNIL a, d'ores et déjà, proposé une méthodologie en ce sens[60].

À l'issue de la conduite de cette analyse d'impact, si cette dernière fait apparaître des risques importants pour les personnes, le responsable de traitement devra alors consulter l'autorité de protection des données. Si l'autorité de contrôle estime que le traitement envisagé pourrait présenter un risque, notamment si le responsable du traitement n'a pas suffisamment identifié ou atténué ce risque, ladite autorité fournit par écrit, dans un délai maximum de huit semaines[61] à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant[62]. Les délais d'examen de la demande peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations demandées.

Incidemment, le mécanisme d'*accountability*, se voit accompagné par l'affirmation de grands principes que sont le *privacy by design* et le *privacy by default*[63]. Ces nouvelles obligations imposent la prise en compte dès l'origine des impératifs en matière de protection des données dans les projets. Il est vrai que, pour l'heure, la question de la *privacy* est souvent perçue comme un élément périphérique à la conduite de nouveaux projets.

L'instauration d'une telle obligation, doit nécessairement conduire à injecter les enjeux en termes de protection des données dès les premières phases de conception et non plus, comme c'est encore souvent le cas, au moment de la mise en production.

En pratique, le respect de l'obligation de *privacy by design* devra conduire le responsable de traitement à prévoir des mesures techniques ou opérationnelles permettant de garantir le respect des obligations issues du règlement. Si ce dernier évoque explicitement la pseudonymisation et la minimisation, on pourrait aussi penser, notamment, à des procédés automatisés permettant de fixer la durée de conservation des données et incluant des fonctionnalités de purge automatique, en encore à l'adoption de procédures organisationnelles dans le cadre de l'exercice des droits des personnes.

La quasi-suppression[64] des formalités à accomplir auprès du régulateur[65] n'est pas sans conséquences. En effet, l'approche de la conformité fondée sur la responsabilisation de l'entreprise est sans doute celle qui aura le plus de conséquences pratiques à la fois techniques et organisationnelles. Il est vrai que le mécanisme de déclaration/demande d'autorisation avait connu des limites tant en termes d'efficience que de délai de traitement[66].

Il n'en demeure pas moins que ce grand bouleversement devra être digéré par les entreprises dans un délai très court. Le règlement entrant en application le 25 mai 2018, il en reste désormais que peu de temps pour adapter les processus et les organisations aux nouvelles obligations qu'il instaure et ce, alors que dans le même temps, le Groupe de l'article 29 s'attelle à tenter de préciser le contour de ces nouvelles obligations[67] qui demeure parfois encore flou.

Enfin, on notera que la proposition de règlement « *vie privée et les communications électroniques* »[68] diffusée le 10 janvier 2017 comporte un article 39-4 prévoyant que le contrôleur européen de la protection des données[69] établit et publie une liste des opérations de traitement soumises à l'obligation d'effectuer une étude d'impact. ■

59. Le règlement évoque notamment les traitements impliquant un profilage des individus, le traitement massif de données sensibles ou de données relatives à des infractions ou mesures de sureté, ou encore « *la surveillance systématique à grande échelle d'une zone accessible au public* ». Les autorités de contrôle nationales gardent toute latitude pour ajouter des typologies de traitements devant nécessairement faire l'objet d'une étude d'impact.

60. Voir : https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil. La méthodologie proposée repose sur la méthode Ebios. La mise en œuvre pratique demeure cependant particulièrement complexe pour le profane.

61. Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement. En cas de prolongation du délai, l'autorité en informe le responsable du traitement dans un délai d'un mois à compter de la réception de la demande de consultation - Art. 36-2 du règlement.

62. À cette occasion, l'autorité peut utiliser les pouvoirs d'enquête de l'article 58 du règlement.

63. Art. 25 du règlement.

64. Reste le cas dans lesquels l'étude d'impact fait apparaître un risque important pour les données des personnes qui n'a pas pu être couvert.

65. Il est vrai que la conformité basée sur la réalisation de formalités préalable avait montré ses limites.

66. On notera à ce titre que le considérant 89 du règlement évoque explicitement l'échec de la protection des données de la défunte directive 95/46 fondée sur la réalisation de formalités préalables.

67. Le G29 a ainsi publié le 15 décembre 2016 des lignes directrices et questions-réponses sur « *le droit à la portabilité des données, le Délégué à la protection des données ou "DPO" et l'Autorité chef de file* ».

68. Règlement *e-privacy*, appelé à succéder à la directive du même nom.

69. Créé par l'article 53 de la proposition de règlement *e-privacy*. Ce contrôleur est chargé de surveiller et d'assurer l'application des dispositions du droit de l'Union relatives aux données à caractère personnel.