TAlone

Le RGPD : nouveau droit de la protection des données personnelles

26 avril 2020

Table des matières

Peut-être avez-vous entendu parler du **R**ègleement **G**énéral sur la **P**rotection des **D**onnées, en tant que personne ou parce qu'il vous intéresse au niveau de votre structure. Dans ce tutoriel, nous allons aborder les divers aspects de ce fameux RGPD en comprenant à la fois le point de vue de l'utilisateur souhaitant comprendre ses droits, et celui de la structure ayant des exigences beaucoup plus pointues. Aucun pré-requis n'est nécessaire afin de comprendre ce cours, car il est destiné a être accessible au plus grand nombre.

Première partie

Historique et application des lois concernant les données personnelles

I. Historique et application des lois concernant les données personnelles

La France a été pionnière en Europe quant à la protection des données liées à la société de l'information : sa première loi sur la protection des données personnelles date de 1978, soit quarante ans avant l'adoption européenne du règlement général de protection des données (qui est l'objet de ce cours). Je vous propose ici un petit panorama des différentes évolutions de la réglementation sur le sujet en France, avant de proposer une introduction au RGPD, objet de ce cours.

I.1. Petit historique législatif de la protection des données personnelles en France

Cette partie est susceptible de ne pas intéresser les européens non-français ; si cet historique ne vous intéresse pas, vous pouvez passer à la partie suivante sans problème particulier, et je ne parlerais alors plus que du droit européen.

I.1.1. Historique de la loi de 1978

Avant 1978, aucune loi ne régit, en France, la conservation informatisée de données ; cela s'explique par l'ancien système de stockage entièrement mécanique (mécanographie) ; on notera toutefois que des doutes sont émis dès 1970, année où un député, en avance sur son temps, propose la création d'un « tribunal de l'informatique », mais cette idée sera temporairement abandonnée.

C'est en 1974 que le journal *Le Monde* révèle un scandale de taille : le projet SAFARI[1], initié par l'INSEE, consistant à informatiser les fichiers régionaux d'état civil pour les rendre nationaux – ce qui pourrait, selon ses opposants, permettre le fichage des français – ainsi que de les interconnecter avec le fichier des cartes d'identités et d'assurance vieillesse – dans un premier temps, le projet sera modifié ensuite, et n'aboutira finalement pas.

Suite au tollé provoqué par l'article du *Monde* – qui jugea le projet trop vaste et permettant le fichage des français, le nouveau président Valéry Giscard d'Estaing décide la création d'un organisme de contrôle des données personnelles dans la société de l'information : la CNIL, et avec elle est promulguée une loi majeure, la loi de 1978 dite « Informatique et libertés ».

I.1.2. Les atouts de la loi

Cette loi est, comme je le mentionnais en introduction, très en avance pour son époque, la France étant le premier pays européen à légiférer aussi profondément sur le sujet. Le cadre d'utilisation de l'informatique est posé très strictement dans l'article premier :

L'informatique doit être au service de chaque citoyen[2]

C'est en effet de cette phrase que découle le reste du texte, qui pose la définition de la donnée à caractère personnel – définition d'ailleurs sensiblement identique à celle du RGPD. Il pose aussi un principe toujours de rigueur : aucun traitement informatisé ne peut constituer l'unique fondement d'une décision de justice (impossible de condamner quelqu'un uniquement car il apparaît dans un traitement). Par ailleurs, la loi pose les conditions du traitement automatisé de données à caractère personnel, et mets en place quatre droits fondamentaux[3] :

— le droit d'information : chacun peut être informé des traitements dont ses données font l'objet, cet article est applicable en toutes circonstances, même aux cas relevant de la sécurité nationale ;
— le droit d'accès : plus complet que le droit d'information, il permet à chacun d'accéder aux informations qui sont conservées sur lui, il est toutefois interdit d'en faire usage dans certains cas ;
— le droit de rectification : chacun peut demander à faire corriger les données stockées le concernant ;
— le droit d'opposition : chacun peut s'opposer à faire l'objet d'un traitement, pour un motif légitime (le démarchage commercial est reconnu par la loi comme motif légitime).

Ces droits se retrouveront, amplifiés et adjoints à d'autres, dans le RGPD.

I.1.3. Une modification majeure en 2004

En 2004, deux facteurs[4], nommément le début de la marchandisation des données (qui étaient auparavant uniquement confiées à l'État) et la traçabilité (le fait que de plus en plus de traces informatiques sont laissées au quotidien), poussent le législateur à réviser la loi de 1978. En France, cette fois en retard sur l'Europe (qui pousse la directive correspondante en 1995), le contrôle *a priori* de la CNIL, devenu trop encombrant, est transformé en un contrôle *a posteriori*, mais bien plus contraignant, en effet, icelle est maintenant capable de prononcer des sanctions[5] :

— injonction à cesser le traitement ;
— retrait de l'autorisation de traitement ;
— suppression de certaines données ;
— sanction pécuniaire pouvant aller jusqu'à 150 000 € pour les contrevenants.

La nouvelle loi met aussi en place un nouveau système relatif à la déclaration des fichiers et traitements ; toute structure souhaitant effectuer un traitement de données à caractère personnel ou stocker ces données doit effectuer une déclaration à la CNIL, sauf dans certains cas (mais la déclaration devient la norme). On note toutefois que l'État devient soumis au même régime de déclaration simple, alors qu'il était auparavant soumis à une demander d'autorisation, de par la nature très personnelle des données qu'il collecte.

I.1.4. Une loi comportant de nombreuses failles

Ces nouvelles formalités de déclaration vont poser de nombreux problèmes tant pour l'État que pour les structures privées : l'État est sujet à un contrôle peu strict, quand les entreprises n'ont aucune liberté dans la gestion de leurs données personnelles.

De plus, la loi ne protège pas contre de nombreux risques, en effet, la menace sécuritaire est de plus en plus importante et l'État se demande quel est le juste équilibre entre sécurité et liberté ; la loi « Informatique et libertés » commence alors à être attaquée de toute part, en excluant de nombreux fichiers de son champ d'application (fichage des terroristes, notamment).

L'exposition volontaire de soi reste aussi un problème majeur dans la société et rien n'empêche ou ne protège les personnes contre ce phénomène de mise en avant de soi-même, et de publication volontaire d'informations, qui étaient auparavant récoltées à l'initiative d'un organisme ; cette exposition implique une formation des personnes à l'hygiène numérique, avec une sensibilisation dès le plus jeune âge.

Alors que les enjeux se multiplient et que les appareils connectés croissent de manière exponentielle, la loi ancienne ne fait pas le poids face aux nouveaux acteurs, certains étant même prêts à payer les amendes de la CNIL (d'un montant de 150 000 €, 3 millions depuis octobre 2016[6], ce qui n'est rien pour une multinationale), plutôt que de respecter les droits des internautes.

1. L'article intégral peut être trouvé sur le site de l'AFCDP
2. L. n° 78-17, 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés (abrégée ci-après L. I&L), art. 1er
3. L. I&L, art. 38 et suivants
4. Conseil d'État, Jean-François T., Isabelle F.P., Internet et les réseaux numériques, 2 juillet 1998, Documentation Française, 193 p., ISBN : 978-2-11004-102-1
5. L. I&L, art. 45 et suivants
6. L. n° 2016-1321, 7 octobre 2016, pour une République numérique, art. 65, NOR : ECFI1524250L

I.2. Qu'est-ce que le RGPD ?

I.2.1. Historique de la création du RGPD

En janvier 2012, la Commission européenne, consciente de l'absence de consensus sur la protection des données personnelles dans l'ensemble des pays de l'Union, et jugeant le sujet important, décide de rédiger un règlement sur le sujet. De nombreux pays membres sont consultés, et un premier jet du règlement est proposé par la Commission européenne en novembre 2013 [7].

Le texte commence alors à être discuté le 11 mars 2014 par le Parlement européen, qui le modifie, et l'adopte le jour suivant en première lecture [8]. Les négociations se poursuivent rapidement, entre la Commission européenne, le Parlement européen et le Conseil de l'UE, qui aboutiront au texte final le 15 décembre 2015.

Comme vous le voyez, la procédure d'adoption de ce texte – comme souvent en Union européenne – s'est étalée sur une longue période durant laquelle les divers acteurs (États, entreprises et citoyens), ont pu participer au processus de création, le tout afin d'essayer d'obtenir un texte équilibré, à la fois protecteur des personnes, et laissant une certaine liberté aux entreprises et administrations publiques.

I.2.2. Dispositions du règlement

Pour commencer sur les nouvelles dispositions du règlement, il faut d'abord bien comprendre la notion de cadre harmonisé : désormais, toute l'Union est soumise aux même règles, ce qui facilite la circulation des données personnelles à travers l'UE. Pour les données en dehors de l'Union, le règlement est très strict également, puisque celles-ci sont soumises au règlement dans de très nombreux cas.

Concrètement, et nous le verrons en détail par la suite, toute donnée concernant *un citoyen* européen, même traitée hors union, est dans le champ d'application du règlement ; c'est un cadre très large et protecteur pour les Européens. Notons d'ailleurs que je viens, sans même le vouloir, de définir le cadre : ce règlement ne concerne que les *citoyens*, il n'est aucunement applicable aux personnes morales, mais uniquement aux personnes physiques.

Maintenant que les champs d'application sont bien définis, voyons les dispositions du règlement ; j'aimerais d'ailleurs citer, comme je l'ai fait pour le droit français, la phrase dont découle tout le reste du règlement :

Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel[9]

Pour les structures (notons qu'en droit européen, les administrations sont inclues dans ce terme, par conséquent, le droit d'exception antérieur est aboli) traitant de la donnée personnelle, le principe de déclaration obligatoire à la CNIL est transformé en principe de responsabilité, permettant bien plus de souplesse, mais augmentant les sanctions. L'idée est que la structure traitant les données personnelles doit être en mesure de démontrer que les principes de protections sont respectés, et la CNIL pourra contrôler la structure de manière inopinée ; le contrôle, déjà partiellement effectué *a posteriori*, l'est maintenant intégralement, puisque la CNIL ne vérifie rien avant contrôle. En cas de délit constaté lors du contrôle, les amendes sont désormais dissuasives, puisqu'elles peuvent aller jusqu'à 4 % du chiffre d'affaire mondial de l'entreprise[10], une belle somme.

A titre de comparaison, cette règle des 4 % de chiffre d'affaires appliquée au réseau social Facebook nous donne, pour l'année 2017, plus d'un milliard et 300 millions d'euros.

En ce qui concerne les utilisateurs, leurs droits sont renforcés, avec notamment l'arrivée du consentement « explicite » : le traitement des données personnelles est soumis à un consentement qui ne peut être forcé ; particulièrement, l'accès au service ne peut être conditionné à acceptation de traitement de données qui n'y seraient pas directement nécessaires.

I.2.3. Les nouveaux droits des utilisateurs

Le règlement consacre aussi aux utilisateurs les droits mentionnés à la partie traitant du droit français, à savoir[11] :

- le droit d'information, remplacé par un principe de « transparence de l'information », assez précisément défini, notamment en ce qui concerne les informations à communiquer ;
- le droit d'accès, qui reste quasiment le même, à ceci près que la durée de conservation doit maintenant être précisée ;
- le droit de rectification, géré de manière identique : tout changement de la part de l'utilisateur doit être répercuté ;
- le droit d'opposition, à la fois complété et fragilisé, pour former un « droit à l'effacement », qui reste finalement peut-être le point le moins protecteur de la nouvelle législation, en cela qu'il ne prévoit que six cas ouvrant droit à opposition.

A ces droits existants précédemment, le RGPD en créé deux nouveaux :

- le droit à la limitation du traitement[12], qui est une sorte de droit à l'effacement allégé, qui permet de laisser ses données à la structure responsable du traitement, mais de lui demander de les marquer pour limiter leur utilisation future[13] (c'est un droit complexe, nous le reverrons) ;
- le droit à la portabilité[14], fruit d'une longue bataille des associations de défense des droits des citoyens ; il permet à chacun de demander l'intégralité des données à caractère personnel les concernant. Ces données doivent être transmises « dans un format structuré, couramment utilisé et lisible par [une] machine », et il est autorisé d'aller mettre ces données dans un autre traitement, sans que le responsable du premier (celui à qui on demande la portabilité) ne puisse s'y opposer.

7. Texte déposé A7-0402/2013 , 22 novembre 2013, 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
8. Parlement européen, CRE des 11/03/2014 et 12/03/2014
9. Règl. (UE) n° 2016/679 du Parlement européen et du Conseil, 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 (dit ci-après « RGPD » ou « Règlement »), art. 1er, objet et objectifs
10. RGPD, art. 83
11. RGPD, chapitre III, sections 2 et 3
12. RGPD, art. 18
13. RGPD, art. 4 (particulièrement définitions)
14. RGPD, art. 20

I.3. Quelques formalités d'organisation

I.3.1. Les piliers du Règlement

Le RGPD abandonne les formalités auprès de la CNIL, il supprime en tout cas leur rôle prépondérant en amont du traitement des données ; ces formalités sont remplacées par une principe d'« Accountability », c'est-à-dire de responsabilité pour les structures traitant de la donnée. Ces nouvelles règles imposent d'adopter une démarche destinée à prouver la conformité avec la loi d'une entreprise concernée, qui pourra être contrôlée à tout moment.

Les outils de preuve de la conformité sont de plusieurs ordres, et forment les piliers de l'application du RGPD[15] ; ces cinq piliers doivent être mis en place pour créer un cycle vertueux de la donnée, et se mettre ainsi en conformité avec le Règlement. Le premier pilier est la bonne gestion de la gouvernance, avec une attribution correcte des rôles aux différentes personnes concernées ; il est pour cela recommandé de mettre en place un tableau de responsabilité et de gestion des tâches, afin de savoir qui doit faire quoi (ce tableau est appelé « matrice de conformité »), et le DPD doit être l'élément central de ce tableau, celui à qui on réfère de toutes les démarches effectuées.

Le second pilier consiste en une connaissance experte des règles en matière de traitement de données, ce qui passe aussi en règle générale par le DPD – que nous mentionnerons juste après, avec une bonne capacité d'adaptation à la pratique, car les règles ont parfois de multiples interprétations. Pour faire la jonction entre cette connaissance des règles et leur mise en pratique, il est nécessaire d'effectuer des analyses d'impact ainsi que divers documents d'étude *a priori* du projet.

I.3.2. Éléments de preuve de la conformité

Une fois toutes les bonnes pratiques mises en place, par les trois piliers mentionnés précédemment, il faut s'organiser pour document ces pratiques et s'assurer d'être en mesure de prouver la conformité au Règlement ; c'est l'objet des deux derniers piliers, qui constituent des preuves de forme et de fond de la conformité.

Pour ce qui est des éléments de forme assurant la conformité, il est nécessaire d'effectuer une cartographie des traitements, avec une analyse précise des données, systèmes, flux, prestataires, modalités de conservation et risques mis en jeu ; ces éléments doivent montrer une analyse complète du traitement *a priori*, afin que l'autorité de contrôle puisse s'assurer de la bonne foi de la structure correspondante, qui à défaut de la défausser de charge, lui évitera au moins un procès.

Ces éléments de forme sont complétés par la tenue obligatoire[16] d'un registre des traitements, contenant diverses informations, dont celles transmises à l'utilisateur que nous verrons dans

la partie suivante, ainsi qu'une description des catégories de personnes concernées, la liste des entités auxquelles les données ont été transmises, la liste des sous-traitants et enfin une description générale des mesures de sécurité et de confidentialité mises en place au niveau technique.

Pour terminer sur ces cinq piliers, la preuve de la conformité doit être appuyée d'éléments de fond, cela concerne – et nous en reverrons la plupart – les contrôle et audits, au quotidien, en interne et pour les prestataires, le *reporting* effectué par le DPD et le suivi des conseils et injonctions données par le DPD, l'autorité de contrôle ou l'autorité judiciaire.

I.3.3. Le rôle du DPD

Le Règlement mentionne le **D**élégué à la **P**rotection des **D**onnées comme un élément central du processus de mise en conformité : il est chargé de nombreuses missions, qui peuvent être effectuées pour le compte d'une structure ou d'un ensemble de structure agissant conjointement dans un groupement d'entreprises ; ses missions sont, notamment[17] :

- informer et conseiller le responsable du traitement ainsi que les employés de la structure pour laquelle il travaille, en particulier sur leurs obligations au regard du Règlement, et d'éventuelles autres dispositions européennes ou nationales concernant la protection des données ;
- contrôler le respect des dispositions qu'il a eu mission de mettre en pratique, pour le compte de son entreprise ou groupement d'entreprise, et concernant les divers sous-traitants ; ainsi, il a pour mission de vérifier le bon déroulement des procédures de contrôle ainsi que le résultat des audits internes ;
- dispenser des conseils, sur demande, en ce qui concerne les PIA et la mise en place d'une PSSI, deux notions que nous étudierons en détails dans ce cours ;
- coopérer avec l'autorité de contrôle, pendant et hors périodes de contrôle, et faire office de point de contact entre la structure et l'autorité compétente en niveau national sur toutes les questions relatives au traitement.

Le rôle du DPD est donc double : il agit en amont et en aval de la mise en conformité, pour conseiller et vérifier que tout soit en règle. Conséquemment, il doit disposer de nombreuses compétences dans des domaines très divers, principalement le droit, mais aussi l'informatique, la sécurité, les ressources humaines, la communication… Pour ceux d'entre vous souhaitant devenir DPD, ce cours peut être une bonne introduction, mais pas une formation à part entière, il vous sera nécessaire d'aller directement lire le Règlement pour y découvrir les points occultés dans ce cours, et d'acquérir de bonnes notions, d'informatique particulièrement.

Notons le statut particulier du DPD au sein de l'entreprise : il doit agir en toute indépendance, ce qui signifie qu'il doit être libre de ses actions dans le cadre de sa mission, ne pas avoir de conflits d'intérêts (un DPD ne peut pas être responsable du traitement, par exemple) et est protégé au sens qu'il ne peut pas faire l'objet de sanctions disciplinaires liées à son activité[18] (il peut dire ce qui est nécessaire sans que son statut, sa paie, ou quoi que ce soit d'autre ne soit

affecté).

15. Anne Debet, Jean Massot, Nathalie Metallinos, La protection des données à caractère personnel en droit français et européen, 2015, L.G.D.J., coll. Les Intégrales, 1296 p., ISBN : 978-2-35971-093-9
16. RGPD, art. 30
17. RGPD, art. 39
18. G29, avis n° 1/2016, 5 avril 2016, WP 243

I.4. La première question : À quoi s'applique-t-il ?

J'aimerais, avant tout, aborder une question qui devrait intéresser chacun, et que nous avons déjà partiellement traitée dans la sous-partie précédente : qui est concerné par ce fameux règlement ? Nous avons déjà vu qu'il pouvait s'appliquer aux données des Européens, même hors Union Européenne, mais il nous faut nous intéresser plus en détails à son champ d'application dans le temps et dans l'espace. Une autre notion importante que nous étudierons est la notion de sous-traitance, qui reste, malgré tous les efforts du législateur, assez complexe à appréhender.

I.4.1. Qui doit l'appliquer ? Au profit de qui ?

Soyons clairs sur ce point, le Règlement s'applique à tous, enfin presque tous, puisque qu'il ne concerne que les personnes morales : est exclu de son champ d'application « tout traitement effectué par une **personne physique** dans le cadre d'une activité **strictement personnelle** ou domestique »[19]. Les personnes physiques effectuant un traitement pour le compte d'une personne morale ne sont donc pas exclues du cadre du RGPD. Cette notion d'activité strictement personnelle permets de libérer les éditeurs de petits sites personnels, qu'ils pourront donc administrer sans s'embêter avec des procédures juridiques.

Un autre point important du Règlement : il ne concerne que les traitements de données de personnes physiques[20], les échanges entre personnes morales étant considérées comme purement commerciales.

Certaines entreprises, pour faire traiter leurs données, font appel à des sous-traitants ; le RGPD définit cette notion de sous-traitant comme :

— une personne physique ou morale ;
— qui traite des données à caractère personnel ;
— pour le compte du responsable du traitement.

Dans ce cas précis de sous-traitance, la définition de la responsabilité est floue au niveau du RGPD (le sous-traitant doit présenter « des garanties suffisantes », techniques et organisationnelles quant à l'application du Règlement), mais en se basant sur les conclusions du G29[21], il est possible de retenir un faisceau d'indices indiquant qui est le véritable responsable du traitement : il doit être à l'initiative du traitement et en définir la finalité – la première chose à regarder est donc : qui souhaite ce traitement ? Le responsable faisant appel à un sous-traitant doit aussi, pour que sa responsabilité soit engagée, avoir une influence de droit *ou de fait* sur le traitement ; cette influence peut donc être stipulée par contrat ou simplement constatée.

La responsabilité du sous-traitant sera, quant à elle, appréciée par son autonomie et son pouvoir décisionnaire quand au traitement, ainsi que par la possession des moyens matériels,

humains, techniques et organisationnels du traitement ; on remarque que dans de nombreux cas, la responsabilité du « simple » sous-traitant ne peut être engagée, j'entends par ici que le sous-traitant doit avoir une réelle liberté d'agir pour qu'il puisse être responsable du traitement. Par conséquent, c'est l'entreprise qui demande la sous-traitance qui doit traiter les requêtes des utilisateurs, et qui doit justifier du bon déroulement du traitement en cas de demande de la CNIL, mais le sous-traitant doit s'assurer du respect des obligations de sécurité et de confidentialité.

Signalons enfin que si la responsabilité du sous-traitant est établie *a posteriori*, le responsable du traitement peut réclamer au sous-traitant le remboursement d'une réparation versée antérieurement suite à la plainte d'un utilisateur, dans la limite des délais légaux.

I.4.2. Quelles données sont concernées ?

Nous ne cessons depuis le début de ce cours d'évoquer les notions de donnée personnelle et de traitement, mais nous n'avons jamais défini ces notions de façon claire ; je vais donc me permettre de lister les conditions définissant un traitement :

- il s'agit d'une opération ou d'un ensemble d'opérations ;
- effectuées **ou non** à l'aide de procédés automatisés, ce qui signifie qu'un stockage papier d'informations, qui seraient consultés de temps à autres, entre dans cette définition ; le RGPD ne nous parle pas uniquement de traitements informatisé, même s'ils en sont l'objet majeur ;
- appliquées à des données à caractère personnel. Et pour être plus précis sur cette notion de donnée à caractère personnel, même si la définition relève du sens commun, elle est « toute information se rapportant à une personne physique identifiée ou identifiable », incluant les personnes identifiables par un identifiant ou un numéro ou même un faisceau d'éléments concordants[22].

Pour quelques exemples de données à caractère personnel, on pourrait citer, permettant une identification directe le nom, le prénom ou encore le numéro de sécurité sociale ; de manière indirecte, il y a une adresse, une photographie, un numéro de téléphone (à la limite de l'identification directe) et de manière très indirecte, un enregistrement vocal, par exemple – qui est effectivement une donnée personnelle, d'après la CNIL .

Deux choses importantes sont à noter : les données peuvent être à caractère personnel même si elles sont publiques ; pour que ces données ne soient plus considérées comme personnelles, elles doivent être anonymisées – et non pseudonymisées[22], de manière à rendre impossible toute identification de la personne concernée.

I.4.3. Les conditions d'application dans l'espace et dans le temps

Nous avons déjà mentionné l'application dans l'espace peu avant, il est maintenant nécessaire de la préciser ; nous savons déjà que la loi s'applique pour toute donnée concernant un citoyen européen, plus spécifiquement, il faut que le responsable du traitement, ou le sous-traitant soit

établi sur le territoire de l'EU, ou alors pour les personnes se trouvant sur le territoire de l'Union, lorsque l'entreprise :

> — offre des biens ou des services [aux] personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou
> suit le comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.
>
> Source : article 3 du RGPD

Il faut comprendre que si les personnes dans l'Union ont leurs données personnelles traitées suite à une prestation, facturée ou non, l'entreprise effectuant le traitement tombe sous l'objet du Règlement, ainsi que si elle suit le comportement de ces personnes, même sans fourniture d'une quelconque prestation (c'est le cas des régies publicitaires, par exemple).

En ce qui concerne l'application temporelle du RGPD, icelle est définie jusqu'à expiration de la durée de conservation définie (le « droit à l'oubli » dont nous parlerons plus loin), ou, à défaut, jusqu'à ce que les données ne soient plus nécessaires.

Un utilisateur peut exercer ses droits sur des données qui n'ont pas été supprimées, qu'elles ne l'aient pas été car elles sont encore utilisées, par négligence, ou car elles sont archivées (notons que la durée d'archivage fait partie de la durée de conservation).

Maintenant que les questions concernant la protection des données personnelles sont posées pour les particuliers et entreprises, le cours se sépare : une partie, concernant les droits des utilisateurs, est recommandée à tous ; une seconde partie, sur la gestion du RGPD dans une structure (principalement en entreprise) est plus pointue et plutôt réservée à ceux ambitionnant de devenir DPD (c'est-à-dire responsable des données personnelles, au nivau juridique et technique), ou à s'informer plus amplement à ce sujet.

19. RGPD, art. 2
20. RGPD, art. 1er, cf. la phrase mentionnée ci-avant
21. G29, avis n° 1/2010, 16 février 2010, WP 169
22. Si vous souhaitez savoir pourquoi, je vous invite à écouter Benjamin Bayart , au sujet de l'anonymisation, et la réponse d'Axelle Lemaire sur son opposition auprès de l'Europe

Deuxième partie

Les principes généraux

Nous voici dans cette première partie, qui abordera le nouveau droit des personnes régi par le RGPD ; cette partie est conseillée à la lecture pour tous. Nous verrons ainsi les grands principes du Règlement : principes du traitement et droits fondamentaux des personnes en faisant l'objet.

II.1. Les principes du traitement

Commençons par mentionner l'alinéa du texte de loi structurant cette partie, où les trois principes sont posés clairement, même si nous les traiterons dans un ordre différent :

> Les données à caractère personnel doivent être [...] traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)
> Source : Article 5 du RGPD

Aussi, laissez-moi définir un concept qui sera réutilisé par la suite, la finalité du traitement : c'est en réalité l'objectif du traitement, sa raison d'être ; sans finalité, un traitement ne peut exister (ou alors il est illicite), selon le droit européen.

II.1.1. Principe de collecte loyale

Le principe de collecte loyale existe déjà depuis longtemps en droit français ; il est en effet mentionné à l'article 226-18 du Code Pénal, qui interdit la collecte de données personnelles « par un moyen frauduleux, déloyal ou illicite ». Une jurisprudence existe donc déjà à ce sujet, on sait ainsi[1] qu'est déloyal un traitement consistant, pour une société de recouvrement, à collecter des informations concernant une personne, à partir de ses lettres écrites au propriétaire ou syndic' de copropriété, à l'exception évidente de ses informations de contact usuelles.

Aussi, la jurisprudence française, qui devrait rester applicable suite au RGPD, précise qu'une information librement accessible ne peut pas forcément être librement réutilisée[2], et constitue, sans consentement de l'utilisateur, et hors cas d'exception (je pense ici à la sécurité nationale, ou au traitement effectué par une personne physique), une atteinte au principe de loyauté. PagesJaunes avait en effet « aspiré » les données de millions d'utilisateurs – qu'ils avaient eux-même mis en ligne sur les réseaux sociaux – pour remplir son célèbre annuaire.

Le RGPD, quant à lui, définit clairement ce principe, mais hors de son champ de définitions[3] : il précise que la personne concernée doit être informée de l'existence et des finalités du traitement ; entre aussi dans cette définition le fait de porter à la connaissance de l'utilisateur les conséquences pour lui s'il refuse ce traitement. En outre, est aussi précisée la possibilité de recourir à des icônes pour faciliter la compréhension par l'utilisateur du traitement et de ses conditions ; cela montre que le Règlement n'est pas formel concrètement : la seule chose qui importe est l'information de l'utilisateur – notons que l'utilisation unique d'icônes ne saurait par contre, à elle seule, informer suffisamment l'utilisateur.

Plus loin, le RGPD, après avoir mentionné l'obligation de ce principe de loyauté, mentionne, sans les attribuer directement au principe, deux obligations qui y sont liés : l'obligation de finalités « déterminées, explicites et légitimes »[4] (c'est le principe de proportionnalité), ainsi qu'un traitement « adéquat, pertinent et limité »[4] des données. Ces nouvelles définitions se passent de commentaire, et permettent déjà de bien mieux cerner le principe de collecte loyale.

Pour revenir un instant sur le principe de proportionnalité, qui est à la fois lié et considéré indépendamment du principe de loyauté[5] : il s'apprécie au cas par cas, en fonction des règles applicables, c'est donc principalement la jurisprudence à venir qui nous donnera les cas particuliers où il est respecté ou non. Un exemple n'est jamais de refus, on pourrait ainsi citer le Code du Travail[6], en matière de traitement dans un cadre RH, qui prévoit des dispositions de lutte contre les discriminations, un fichage ethnique est donc une collecte disproportionnée, en vertu des textes applicables.

Il convient de faire légalement attention aux collectes indirectes, comme les adresses IP qui sont collectées et stockées, généralement avec des données temporelles et de connexion, par les prestataires d'hébergement. Ces données sont pour la plupart (sauf à être anonymisées avant stockage) soumises au même RGPD que les traitements « volontaires ».

Pour terminer, et comme le sujet est très dense, je vous recommande de regarder les recommandations de la CNIL à ce sujet, par exemple ici pour le commerce et le marketing .

II.1.2. Obligation de transparence

> Cette partie sera plus courte que les autres, en effet, j'ai préféré, pour des raisons de simplicité, traiter cette obligation en deux fois : d'une part, cette partie, qui mentionne le principe général de transparence, et la partie sur la sécurité et la confidentialité, qui comporte un volet de transparence.

Comme je le précisais en introduction, une obligation de transparence incombe au responsable du traitement ; cette obligation se compose en partie du droit à l'information, qui consiste à permettre à l'utilisateur de demander à tout moment d'être informé sur les traitements dont ses données personnelles font l'objet[7], ainsi que de pouvoir être informée de la finalité et des modalités du traitement. Je reparlerais de ce droit plus en détails dans la partie prévue à cet effet, mais sachez qu'en pratique (hors du droit de contexte du simple RGPD), il ne peut, sauf rares exceptions, être opposé à une personne, même dans des cas de sécurité nationale – avec des subtilités toutefois, comme le fichier des fichés S, où il se transforme plutôt en droit au contrôle externe (la personne peut demande que soient vérifiés que le traitement dont elle fait l'objet sont légaux, mais ne peut le vérifier elle-même).

Le Règlement énumère un ensemble d'informations devant être obligatoirement communiqué aux personnes concernées ; si la collecte est directe – c'est-à-dire qu'elle est effectuée directement auprès de l'utilisateur, il faut fournir[8] :

— l'identité et coordonnées du responsable du traitement et du DPD ;
— si les données sont transmises à un tiers, l'identité de ce tiers ;

1. Cass. Crim., 3 nov. 1987, n° 87-83429
2. CE, 9 et 10ème chambre, 12 mars 2014, n° 353193, dite « PagesJaunes »
3. RGPD, considérant 68
4. RGPD, art. 5, considérant (b) et (c)
5. Il est indépendant sur la forme (séparé au niveau législatif), mais poursuit un même objectif de fond
6. C. trav., art. L1132-1 et autres

— la finalité du traitement et sa base juridique (extraite du principe de licéité que nous verrons après) ;
— l'existence d'un transfert hors EU dans certains cas (nous le reverrons) ;
— la durée de conservation des données (droit à l'oubli) ;
— un rappel des différents droits des utilisateurs (les six fondamentaux et le droit au recours effectif).

Les informations à fournir varient légèrement si elles ont été collectées de manière indirecte, le dernier point ci-dessus est en effet inapplicable et remplacé la mention de la catégorie des données concernées ainsi que de la source de ces données.

Pour terminer sur ce principe de transparence, il est constitué d'un dernier volet concernant une certaine transparence concernant l'utilisation des données : le Règlement rappelle[9], particulièrement, le droit de ne pas faire l'objet d'une décision fondée **exclusivement** sur un traitement automatisé (limitant ainsi le profilage, c'est-à-dire l'analyse informatisée d'un comportement) ; ce principe est l'un des seuls précisés concernant l'utilisation des données (transparence *a posteriori*).

II.1.3. Licéité du traitement

La licéité du traitement, dernier principe consacré par le droit nouveau, est mentionnée juste après la liste des trois principes[10], et consiste en une liste à puce précisant les cas de licéité du traitement. Le premier cas est plutôt simple : il définit le traitement comme licite dès lors que l'utilisateur y a consenti, pour une ou des finalités définies et spécifiques – ce concept de spécificité est très important, vous l'avez peut-être remarqué si vous utilisez Facebook : pour chaque finalité, et pour chaque donnée collectée, le site demande maintenant un consentement précis.

Cette obligation de consentement est novatrice en cela qu'elle consiste en un consentement positif, alors qu'il pouvait avant tout aussi bien être effectué a posteriori du traitement. En pratique, il faut donc que l'utilisateur précise, pour chaque donnée, et chaque finalité, son choix concernant cette donnée personnelle ; ce choix doit consister en un « oui » ou un « non », les anciens sites présumant que vous acceptez une collecte en continuant la navigation sont donc dans l'illégalité.

Notons que le choix de l'utilisateur ne peut en aucun cas altérer son utilisation du service, s'il refuse un quelconque traitement, seules les parties du service directement liées à ce traitement particulier peuvent lui être refusées ; il ne peut en aucun cas être privé d'accès total au service, sauf si le traitement est strictement nécessaire au dit service[11].

Le consentement n'est pas forcément la base légale privilégiée lors d'un traitement de données : pour éviter les contraintes de celui-ci le législateur prévoit de nombreuses exceptions au principe général (de consentement). Le traitement peut ainsi être effectué s'il est nécessaire à l'exécution d'un contrat auquel la personne concernée a souscrit – on pense ici particulièrement aux contrats commerciaux, où le traitement, par exemple, de l'adresse de livraison, est évidemment nécessaire à la réalisation du contrat.

7. RGPD, art. 12
8. RGPD, art. 13
9. RGPD, art. 22

Les autres exceptions sont moins importantes et concernent, dans l'ordre[12] :

— le respect d'une obligation légale : si le responsable du traitement est contraint par la loi à effectuer ce traitement ;
— la nécessité de sauvegarde des intérêts vitaux d'une personne, plus précisément « de la personne concernée » ; il va de soi qu'un hôpital recevant quelqu'un en urgence ne peut lui demander de consentir au traitement préalablement aux soins ;
— la nécessité d'exécution d'une mission d'intérêt public ; c'est probablement l'exception qui suscitera le plus de doute d'interprétation, étant donné que le sens de « mission d'intérêt public » n'est pas défini par le RGPD ;
— la nécessité du traitement « aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers » ; en substance, cela concerne typiquement la justice, qui pourra traiter des informations sur une personne assignée sans son consentement, car la personne qui en assigne une autre en justice possède ici un intérêt légitime.

Je mentionne ici la justice comme ayant un intérêt légitime, mais ce principe peut être appelé par une structure privée et constitue sûrement une des exceptions qui sera la plus utilisée, mais elle est à prendre avec des pincettes pour le moment, étant donné le flou absolu qui règne autour, et l'opposition claire entre les principes, par exemple, du droit français, et le RGPD. La CNIL, en effet, considère la prospection commerciale comme interdite[13], mais le Règlement précise bien que « Le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime »[14], et doit à ce titre être autorisé ; seule la jurisprudence future pourra donc borner correctement cette notion d'intérêt légitime, restreint par la préservation des libertés fondamentales[15].

Cette notion de collecte loyale des données personnelles est un pilier du nouveau droit européen, car elle détermine si la collecte peut être autorisée, avant même de parler de son traitement. Elle est donc une question à poser en amont : « Ai-je le droit de procéder au traitement ? ». Du point de vue des utilisateurs, cette notion peut ne pas paraître indispensable, mais elle est très importante, en effet, si vos données n'auraient pas dû être traitées *a priori*, alors elles ne peuvent continuer à l'être.

10. RGPD, art. 6
11. RGPD, art. 7, alinéa 4
12. RGPD, art. 6, licéité du traitement
13. C. consom., art. L. 121-20-5 ; CPCE, art. L. 34-5 ; voir dépliant CNIL « La publicité par voie électronique »
14. RGPD, considérant 47
15. RGPD, art. 6, alinéa 1.f

II.2. Les six droits fondamentaux

Une directive européenne de 1995 consacrait déjà des droits aux personnes fichées, en raison à l'époque de la crainte d'une surveillance (rappelez-vous du projet SAFARI, notamment). Le droit d'information est alors le plus important d'entre eux. Plus de vingt ans plus tard, le RGPD vient renforcer les droits mis en place par cette directive, et en ajoute de nouveaux, suite à de nouvelles craintes de ne pas maitriser ses données (qui implique une législation plus contraignante).

II.2.1. Le droit d'information et le droit d'accès

Je mentionnais dans la première partie le lien très fort entre le droit à l'information et le principe de transparence : ces deux principes sont effectivement très proches, en cela que l'information à l'utilisateur est une forme de transparence envers lui ; nous avons d'ailleurs déjà traité ce principe de transparence dans la partie précédente, en mentionnant que certaines informations devaient être transmises à l'utilisateur au moment de la collecte des données.

Ces informations, transmises lors de la collecte des données, peuvent aussi être demandées par l'utilisateur plus tard[1], après collecte, et doivent lui être transmises à jour – si le responsable du traitement a changé de coordonnées, par exemple, il faut lui donner les dernières informations, pas celles à jour au moment de la collecte. Une unique exception existe à ce droit d'information[2] : si les données ont déjà été transmises à l'utilisateur, par exemple dans le cas d'un traitement antérieur, il n'est pas nécessaire de lui transmettre ces données à nouveau.

Ce droit d'information est complété, il permet ainsi de demander si vos données font ou ont fait l'objet d'un traitement auprès d'une entité – il est utile si vous souhaitez vérifier que des informations vous concernant ont bien été supprimées, par exemple, ou encore dans le cas où vos données pourraient avoir été traitées sans votre consentement (possible dans certains cas, je rappelle). Il vous suffit de contacter le responsable du traitement (ses coordonnées peuvent normalement être trouvées facilement, à défaut, vous pouvez demander à quelqu'un), et de lui demander si vos données sont traitées, en justifiant de votre identité[1].

II.2.2. Le droit d'accès

En complément du droit d'information, l'utilisateur dispose d'un droit d'accéder aux données personnelles le concernant possédées par un organisme[3] ; il étend le droit d'information en ceci qu'en plus de savoir si une structure traite ses données personnelles, l'utilisateur peut accéder à ces fameuses données, encore une fois sous réserve de justifier de son identité.

1. RGPD, art. 15
2. RGPD, art. 13, alinéa 4 et art. 14, alinéa 5.a

Toute personne, désireuse d'accéder aux données personnelles que vous détenez sur elle, peut effectuer une demande de communication. Elle peut mandater un tiers de son choix[4] si elle le souhaite ; dans ce cas, cette tierce personne doit présenter un écrit contenant l'objet du mandat (exercice du droit d'accès) ainsi que les identités du requérant et du tiers. Le responsable de traitement, ou une personne mandatée par elle et soumise par ailleurs au secret, doit s'assurer de la communication dans un délai d'un mois ; ce délai peut être étendu d'un mois supplémentaire, lorsque la demande est particulièrement complexe ou qu'une grande quantité de données est demandée.

Quelques règles spécifiques s'appliquent : pour les mineurs et les majeurs sous tutelle, ce sont les détenteurs de l'autorité parentale ou le tuteur qui effectuent la démarche[5]. La fourniture orale des informations demandées est tolérée du moment que l'identité du requérant a été démontrée par ailleurs, comme pour la communication dématérialisée ou papier ; aucun frais ne peut être exigé lors de la communication des informations, et la voie de communication d'icelles est libre, si l'envoi est effectué par courrier, les frais postaux incombent donc à la structure.

Il existe certaines exceptions au droit d'accès, en cas de demandes « objectivement abusives », par leurs nombre, leurs répétitions ou leur caractère systématique ; si les données ne sont pas stockées pour des raisons techniques ou si le délai légal de conservation est expiré. Dans les cas de prolongation du délai d'un mois, de demande de frais ou de refus de la demande, la charge de démontrer ces éléments incombe à l'entreprise responsable (au responsable du traitement, en l'occurrence).

II.2.3. Le droit de rectification et le droit à l'effacement

Deux droits se retrouvent combinés ici : le droit de rectification est un droit assez mineur du RGPD, et tient en une seule phrase, que je reproduis ici.

> La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.
> Source : Article 16 du RGPD

Je pense que tout est très clair : un utilisateur dispose du droit de rectifier une information ou d'en ajouter une sans rien justifier, mis à part son identité.

Le droit à l'effacement est bien plus complexe en cela qu'il est limitatif, contrairement à celui de la loi de 1978 ; alors qu'icelle prévoyait des exceptions au principe général, c'est maintenant à l'utilisateur d'expliquer pourquoi il souhaite cet effacement, en mentionnant un des motifs du Règlement, qui sont les suivants[6] :

— les données collectées ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées (le fameux « droit à l'oubli », sur lequel nous reviendrons en détails dans la partie suivante) ;

3. RGPD, art. 15
4. Voir ce qu'en dit un DPD
5. RGPD, art. 8

— l'utilisateur retire son consentement : ce cas n'est applicable que si le consentement était la seule base légale au traitement, il n'est donc pas applicable dans les cas d'exception au consentement que nous avons vus dans la partie précédente, que ces cas d'exception s'appliquent *a priori* – un consentement n'est alors pas demandé, ou *a posteriori* – un consentement a été demandé mais n'est plus nécessaire ;
— la personne s'oppose au traitement – hors des cas de consentement – et le responsable du traitement n'oppose pas de motif légitime et impérieux justifiant que le traitement « prévaut » sur les libertés individuelles de la personne concernée[7] ;
— les données ont fait ou font l'objet d'un traitement illicite, ou doivent être effacées en vertu d'une disposition légale ou d'une exigence judiciaire ;
— les données d'un mineur de moins de 16 ans ont été recueillies sans autorisation parentale[8].

II.2.4. Le droit à la limitation du traitement

Attaquons enfin un droit nouveau, qui n'existait pas dans l'ancienne loi française ; ce nouveau droit est créé pour tendre un peu plus vers la pratique de l'utilisation des données, face à la théorie du droit à l'effacement : une fois les données effacées, elles sont réputées effacées partout au niveau de la structure à laquelle l'utilisateur a effectué sa demande, ainsi que par tous les organismes ayant obtenu ces données par l'intermédiaire de cette dite structure, à condition que le motif invoqué par l'utilisateur s'y applique.

Dans la pratique, on constate que la donnée est difficilement effaçable instantanément, et il y a des cas où il semble préférable qu'elle s'estompe plutôt que de se volatiliser. C'est l'objet du droit à la limitation du traitement, qui vous permet de laisser une structure traiter vos données, tout en lui indiquant d'en restreindre leur utilisation au strict minimum, ce dans l'objectif que la donnée tende vers un effacement total[9].

Ce droit peut être invoqué dans certains cas bien précis, le premier consistant en la présence d'un traitement illégal ; dans ce cas, plutôt que d'en demander effacement, l'utilisateur va demander à exercer son droit à la limitation du traitement, qui est implicitement traité comme un consentement à la conservation de la donnée, doublé d'une injonction de restriction de son usage, qui est soumis au consentement de l'utilisateur[10].

Ce droit peut aussi être exercé lorsque l'exactitude des données est contestée, dans ce cas, le responsable du traitement peut conserver les données mais évite leur traitement, jusqu'à ce qu'il en ait vérifié l'exactitude ou non. Enfin, si la personne concernée par le traitement nécessite ces données pour l'exercice de ses droits en justice, il est possible de demander au responsable du traitement de les conserver sans les traiter.

6. RGPD, art. 17, alinéa 1
7. RGPD, art. 21
8. RGPD, art. 8, alinéa 1
9. RGPD, considérant 129 et 156
10. RGPD, art. 18, qui énumère les cas

II.2.5. Le droit à la portabilité

Pour terminer sur cette partie, voici un droit qui devrait plaire à bon nombre d'utilisateurs, et plutôt déplaire aux structures dont le *business* repose sur la donnée ; ce droit permet à chacun d'obtenir toutes les données qu'il a communiquées à un service, dans un format ouvert et interopérable, dans l'objectif de fournir ce fichier à un autre service qui gérera ses données.

Ce droit est déjà très clair, car le RGPD le définit particulièrement clairement, et car le G29 s'est déjà penché sur son cas[11] ; notons d'abord que ce droit ne s'applique qu'aux informations que l'utilisateur communique à un service, et pas aux informations qui seraient internes au service, ou auraient été recueillies ailleurs ou par un autre moyen. L'utilisateur peut demander à récupérer ses données directement, mais il peut aussi « lorsque cela est techniquement possible », demander à ce que ses données soient directement transmises d'un responsable de traitement à un autre.

Du point de vue des responsables du traitement, le G29 recommande de mettre en place une option directe pour télécharger une archive de ses données au sein de leur service, afin de leur éviter d'être inondés de demandes postales. La sécurité des données, et surtout leur confidentialité, doit aussi être assurée ; nous en reparlerons, mais si un doute suffisant persiste quant à l'identité du demandeur, le responsable peut refuse l'accès aux données.

Le droit à la portabilité diffère du droit d'accès en cela qu'il permet la communication directe d'information entre deux services, qu'il est plus limitatif que le droit d'accès, et que les données obtenues dans le cadre du droit à la portabilité sont bien plus difficiles à comprendre techniquement, alors que le droit d'accès doit fournir les données sous forme simple et compréhensible.

Du côté de l'utilisateur, cela veut dire concrètement qu'il pourra faire transférer, lui-même ou par un intermédiaire, les données qu'il a entrées sur une plateforme ; l'exemple couramment utilisé est celui des plateformes de *streaming* musical (par exemple Deezer), auxquelles vous pourrez demander l'intégralité des artistes que vous avez appréciés, dans un format clair et compréhensible par une autre plateforme musicale (par exemple Spotify), ce afin d'obtenir le « transfert » de ces données vers l'autre plateforme. Lorsque nous parlions ci-dessus d'un transfert direct, il pourrait être possible dans ce cas que Deezer transmette directement les données à Spotify, sans passer par utilisateur, mais sous réserve de son consentement préalable.

Dans la partie suivante, nous nous pencherons en détails sur le droit à l'oubli : icelui est détaché de ces six droits fondamentaux mais il y est en même temps très lié, car c'est lui qui limite le traitement dans le temps, il constitue donc par conséquent un cas d'application du droit à l'effacement – notons que même si je les détache ici, ces droits sont directement liés dans le texte du Règlement (voir article 17, nommé « Droit à l'effacement (« droit à l'oubli ») »).

11. G29, avis WP 242, 13 décembre 2016

II.3. Le droit à l'oubli en détails

Nous le mentionnons dans la partie précédente, le droit à l'oubli est un cas particulier du droit à l'effacement : voyons ensemble ses enjeux, ainsi que la question épineuse de la durée de conservation.

II.3.1. Qu'est-ce que le droit à l'oubli ?

Anciennement, les supports physiques de stockage pouvaient être effacés simplement (destruction du papier, formatage du disque dur, etc) ; depuis l'arrivée d'Internet et l'interconnexion des données, cela est devenu plus complexe à mettre en œuvre, de nombreux acteurs pouvant avoir accès et stocker ces données. C'est la raison pour laquelle le droit à l'oubli a été mis en place : pour effacer des données devenues obsolètes, ou non-nécessaires.

Nous en parlions dans la partie précédente, le droit à l'oubli n'est qu'un cas particulier du droit à l'effacement[1], et concerne en somme une « fin de vie » des données. Les données stockées doivent en effet être soumises à une durée de conservation, bien définie au moment où le stockage commence. Cette durée doit être précisée à l'utilisateur lors du recueil du consentement, si celui-ci est requis ; elle est précisée avec les autres facteurs nécessaires, que nous avons vus précédemment.

Le responsable du traitement est établi responsable de la non-destruction de données qui ne devaient plus être conservées, même si la procédure de suppression est automatique (recommandé), il convient donc pour les entreprises d'effectuer une surveillance quant à l'accomplissement de ce droit à l'oubli. Notons toutefois certaines exceptions au droit à l'oubli, dont certaines sont un rappel de la partie précédente[2] :

- à l'exercice du droit à la liberté d'expression et d'information ; une personne publique ayant commis une infraction ne pourra pas demander à ce que son nom soit effacé de l'article de journal le mentionnant ;
- pour respecter une obligation légale, c'est l'objet de l'archivage intermédiaire, dont nous parlerons ci-après ;
- pour les données présentant un caractère historique, scientifique ou statistique, qui peuvent ne pas être effacées si elles sont anonymisées ou anciennes ;
- pour exercer ses droits en justice, quiconque peut demander à ce que le responsable du traitement conserve la donnée, mais elle ne peut plus faire l'objet d'un traitement.

1. RGPD, art. 17, alinéa 1.a
2. RGPD, art. 17, alinéa 3

II.3.2. La durée de conservation et l'archivage

Le RGPD nous précise que la durée de conservation ne doit pas excéder la durée nécessaire aux finalités du traitement[3], ce qui est peu clair, et laisse les entreprises sur un doute important. C'est pourquoi la CNIL ajoute des précisions concernant ce droit à l'oubli, en mentionnant entre autres que cette durée est variable, et n'est pas mentionnée dans les textes officiels.

Il faut donc déterminer au cas par cas la durée maximale de conservation des données à caractère personnel, en se basant, si possible, sur des textes extérieurs à la protection des données, ou sur des recommandations de la CNIL (par exemple, un mois maximum pour les données de vidéosurveillance).

Outre ces recommandations particulières et liées au type de la donnée, la CNIL propose, pour les responsables de traitement, de mettre en place une organisation relative à la donnée – qui est d'ailleurs l'enjeu majeur derrière le texte du Règlement : mettre en place une organisation globale de la donnée dans l'entreprise. Ce système proposé par la CNIL est basé sur divers niveaux d'archivage, formant un cycle vertueux de la donnée[4] :

- en premier lieu, après que la donnée soit recueillie, elle est en archive courante (ou base active), c'est-à-dire que la donnée est activement utilisée ; dans le cas d'un site d'e-commerce, par exemple, l'adresse d'expédition est en archive courante jusqu'à la livraison du paquet ;
- ensuite, lorsque la donnée n'est plus activement utilisée, elle doit être conservée pour justifier d'obligations légales, on appelle ce stade les archives intermédiaires. Pour reprendre l'exemple du site e-commerce, aucun texte de référence ne mentionne la durée de conservation de l'adresse, mais on pourrait imaginer la fixer à la durée d'exercice possible du droit de rétractation (durée courte), ou une autre durée qui pourrait constituer un fondement légal, réglementaire, contractuel ou conventionnel ;
- enfin, à la fin de la durée définie pour l'archivage intermédiaire, la durée doit être détruite, c'est-à-dire qu'il ne doit rester **aucun moyen** d'y accéder de la part du responsable du traitement. Pour les données présentant un caractère historique, scientifique ou statistique, icelles peuvent ne pas être détruites et sont alors en archives définitives, ce qui signifie qu'elles ne doivent pas faire l'objet d'un traitement régulier (elles peuvent être reprises à la demande d'un historien, par exemple) ; les données doivent alors, la plupart du temps, être anonymisées, ou très anciennes, et ne plus concerner une personne vivante.

Pour l'archivage intermédiaire, la CNIL nous précise que « des mesures techniques et organisationnelles doivent être prévues pour protéger les données archivées », mentionnant à la fois l'accès non-autorisé aux données archivées, même en base active, ainsi que la suppression ou l'altération de ces données aux dépens de l'utilisateur. En cela, elle précise que l'accès aux données stockées doit être tracé, ce qui implicitement veut dire que chaque accès doit être daté, et précisé d'un motif justifiant son accès[5].

3. RGPD, art. 5, alinéa 1.e
4. CNIL, délibération n° 2005-213, 11 octobre 2005, NOR : CNIX0508839X
5. cf. le site de la CNIL

II.3.3. Un cas particulier : le droit au déréférencement

Le droit à l'oubli fait parfois l'objet de décisions spécifiques, c'est le cas d'un principe appelé « droit au déréférencement », et ayant été consacré bien avant que le RGPD entre en vigueur[6]. Il permet aux utilisateurs de demander la désindexation – c'est-à-dire l'effacement de données les concernant auprès d'un moteur de recherche – de n'importe quelle donnée pouvant leur porter préjudice, comme un ancien CV ou une photo de jeunesse, mais aussi de données à caractère racial, religieux et autres[7]. Le déréférencement peut être demandé par le moyen que choisi le responsable du traitement (par voie postale, comme Ixquick, ou en ligne, comme Google et Yahoo).

Attention toutefois, ce droit ne consiste pas pour les utilisateurs à faire effacer une information d'un site web donné, mais simplement d'effacer l'association entre les nom et prénom de la personne concernée et le lien vers ladite page dans un moteur de recherche. L'information reste donc accessible si l'adresse du site est tapée directement dans la barre d'adresse, par l'intermédiaire d'éventuels autres moteurs de recherche à qui l'effacement n'aurait pas été demandé, ou même depuis le moteur auquel l'effacement à été demandé, par d'autres mot-clés.

Ce droit inverse en partie les rapports de force entre l'utilisateur et la plateforme, icelle est en effet obligée de recourir à la demande de l'utilisateur, sauf si l'information ne cause de préjudice à la personne concernée (l'utilisateur peut alors s'y opposer, le plus souvent par un recours gracieux), ou si la suppression de l'information entrave le droit à l'information – remarquons que le premier cas découle en quelque sorte de celui-ci, car s'il n'y a pas de préjudice, alors la liberté d'information est forcément impactée par le déréférencement… d'une information.

En France, le Conseil d'État, saisi en 2017[8] de demandes suite au refus par la CNIL de l'application du droit au déréférencement sur les différentes extensions d'un moteur de recherche (si l'effacement est demandé sur google.fr, doit-il être répercuté sur google.com), demande à la CJUE de trancher la question ; pour cela, il pose les questions suivantes[8] :

- un moteur de recherche est-il directement responsable des données ethniques[7] qu'il diffuse, même si elles sont couvertes par la liberté d'information ?
- Si oui, y-a-t-il des exceptions qui empêchent l'exercice du droit au déréférencement, en particulier concernant les données publiques, ou lors du consentement de l'utilisateur ?
- Si non, quelles sont les limites du droit au déréférencement ? Particulièrement, si le déréférencement est demandé, la légalité des données au regard de la loi du l'Union doit-elle constituer un élément de décision de déréférencement ?
- En tout cas, la liberté d'information est-elle plus importante que le droit à l'oubli, ou une information doit-elle être conservée par un moteur de recherche en toutes circonstances ?
- Enfin, le récit d'un procès est-il soumis au droit au déréférencement, sous réserve que la personne soit explicitement nommée ?

Comme vous le voyez, la question du droit au déréférencement est loin d'être tranchée, malgré son application dès 2014 ; on peut donc supposer qu'il en sera de même du RGPD, qui fera l'objet d'une jurisprudence importante. Soyez donc vigilants et stricts dans votre application du Règlement, et particulièrement de ce droit au déréférencement, dont des questions le concernant

sont encore pendantes devant la CJUE.

Vous voici parés face au droit à l'oubli, qui est, je le rappelle, un des plus importants de cette nouvelle législation européenne.

Le partie suivante, déjà plus technique, abordera des points plus pointus du RGPD, comme la nécessaire sécurité des données, et particulièrement des données sensibles, ainsi que le transfert des données de citoyens européens hors de l'Union Européenne.

6. CJUE, grande chambre, 13 mai 2014, n° C-131/12, ECLI:EU:C:2014:317, dit « Google Spain »
7. Directive (UE) n° 95/46/CE du Parlement européen et du Conseil, 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, art. 8, alinéas 1 et 5 pour la liste des données à caractère particulièrement sensible
8. CE, ass., 24 février 2017, n°s 391000, 393769, 399999, 401258

Troisième partie

Quelques points en détails

Cette partie, qui intéressera sans doute à plus forte raison les entreprises, concerne les points particuliers du Règlement, comme le transfert des données hors Union. Les utilisateurs ne devraient pas s'en faire : ils comprendrons sûrement tout aussi bien ce qui est dit, et pourrons ainsi suivre ce cours jusqu'à sa fin.

III.1. Sécurité et confidentialité des données

Voilà une partie qui s'annonce très dense, étant donné les exigences du RGPD à ce sujet ; nous traiterons de la nouvelle obligation incombant aux structures qui est celle d'assurer la confidentialité des données personnelles. Aussi, en matière de sécurité, nous survolerons – car ces notions pourraient faire l'objet d'un cours complet – les politiques de sécurité des systèmes d'information, maintenant obligatoires, ainsi qu'un concept nommé Privacy Impact Assessment, et consistant à étudier les impacts d'un projet sur la vie privée avant même de le concevoir. Du point de vue des utilisateurs, cette partie consiste à étudier quelles mesures de protections seront appliquées à leurs données, et à comprendre leurs droits à ce sujet.

III.1.1. Présentation générale

Commençons tout d'abord par définir les deux termes qui seront objets de toute cette partie, à savoir :

- la confidentialité est, selon les termes de l'ISO « le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé », il s'agit donc d'un contrôle d'accès indirect, qui s'applique à la fois au niveau physique (contrôler les portes qui mènent aux terminaux) et numérique (contrôler les terminaux eux-mêmes) ;
- la sécurité, quant à elle, est une situation dans laquelle le risque est minimal par rapport à la donnée, il faut pour cela prendre à la fois des éléments de risque, mais aussi évaluer l'importance des données traitées.

Le RGPD regroupe plus ou moins ces deux concepts dans celui de sécurité, pour la raison simple que la sécurité est seule garante de la confidentialité des données, elle est à ce titre la clef de voûte à la fois de la confidentialité et de l'intégrité des données, puisqu'elle empêche leur modification ou leur accès par une personne malveillante.

Pour commencer à parler réellement des dispositions du RGPD, il faut noter que la sécurité et la confidentialité des données sont à prendre de manière globale ; chaque traitement doit faire l'objet d'analyses permettant de prendre en compte la meilleure manière de sécuriser la donnée, en en considérant tous les éléments environnants, qui sont d'ailleurs parfois d'autres données personnelles.

Le principe général est le suivant : nécessité de mettre en œuvre toutes les mesures de protection possibles en fonction de l'état de l'art afin d'assurer la confidentialité, l'intégrité (c'est-à-dire l'exactitude par rapport aux données originales) et la sécurité des données personnelles[1]. Pour cela, le Règlement propose quatre moyens, non-exhaustifs :

— la pseudonymisation des données (une forme d'anonymisation dont nous parlions avant, qui n'en est pas réellement) ;
— la mise en place de chiffrement, c'est-à-dire de mesures techniques permettant que des données éventuellement volées ne puissent être lues ;
— des moyens permettant de rétablir les données en cas d'incident physique ou technique ;
— une procédure visant à tester l'efficacité des mesures mises en place.

Le dernier point est très important et rappelle la liberté laissée à l'entreprise en termes de sécurité : tout est possible en termes de forme, mais il faut en tous cas documenter et tester. Aussi, le RGPD rappelle que la sécurité est forcément basée sur l'équilibre, entre « l'état des connaissances, [l]es coûts de mise en œuvre et la nature, la portée, [le] contexte et [l]es finalités » d'un part, et de l'autre, « [l]es risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ».

Enfin, notons qu'il y a des précautions à prendre pour les sous-traitants : toute personne physique agissant sous l'autorité d'un responsable de traitement ne peut traiter les données que sur ordre direct de celui-ci ; le sous-traitant doit garantir de bonnes conditions de sécurité par contrat, et ne peut faire sous-traiter par quelqu'un d'autre sans y avoir été explicitement autorisé.

III.1.2. Mise en œuvre interne

Beaucoup de formalités internes ici (c'est le but) ; si l'idée vous répugne, fuyez à la partie suivante.

La loi Informatique et Liberté précise[2] qu'il faut mettre en place en interne des précautions utiles, au regard de la nature des données et des risques présentés par le traitement ; cette disposition est reprise par le RGPD[3] et synthétise ce qui a été vu dans la partie précédente. Dans cette partie, le terme « en interne » va nous intéresser particulièrement, car une grande et stricte organisation sera requise pour sécuriser la donnée, et surtout être en mesure de la prouver à la CNIL.

Premièrement, le Règlement mentionne un principe appelé « Privacy by Design », qui constitue à penser à la protection des données dès l'étape de conception, c'est-à-dire dès l'origine du traitement. C'est une démarche à laquelle votre esprit devrait être habitué depuis le début du cours, car l'organisation de celui-ci vous mène à poser des questions de nécessité de traitement. Cette conception avec l'idée de protection des données n'implique pas que le problème s'arrête ici, il faut ensuite interpréter et adapter les règles tout au long des différents traitements, c'est pourquoi il faut pour les structures établir une politique des systèmes d'informations[4], qui soit globale et s'applique dans toute la structure, ou toute le département informatique.

Cette PSSI n'est en réalité pas un unique document, mais est en général constituée [5], d'abord, d'une politique générale, qui se constitue elle-même d'un ensemble de documents précisant le périmètre d'application, les acteurs et leurs missions et les risques concernés ainsi que les modalités de mise en œuvre de la politique, de *reporting* et de contrôle des procédures. Concernant les acteurs, le responsable de traitement est garant ad-hoc de la sécurité des données en tous cas, mais le responsable pratique est en réalité plutôt une personne spécifiquement nommée à

1. RGPD, art. 32

cet effet dans les grandes entreprises, ou un ingénieur en sécurité informatique ; quant au DPD, il n'est comme toujours pas responsable, mais doit conseiller correctement une entreprise lors du processus de mise en sécurité des données.

Peuvent être adjoints à ce document de politique générale diverses politiques spécifiques qui peuvent être présentes dès le départ, ou ajoutées par la suite. On pourrait citer, non-exhaustivement[5] :

— une politique sur la sécurité physique qui définit les procédures à mettre en œuvre pour empêcher un accès physique non autorisé, ou tout dommage ou intrusion dans les locaux hébergeant les données ;
— une politique sur les modalités de traitement de l'information qui précise où sont stockées les données, les modalités de leur destruction, ainsi que les mesures de sécurités logicielles (pseudonymisation, chiffrement, …) ;
— une politique de sauvegarde et d'archivage qui assure l'intégrité et la disponibilité des éléments amenés à être restaurés, et explique le choix des solutions d'archivage (le système en trois archives dont nous parlions).

III.1.3. Notification des failles de sécurité

Le RGPD introduit une notion qui n'existait avant que dans peu de pays européens : l'obligation de notifier les failles de sécurité[6]. L'exigence envers les responsables de traitement est grandissante, et afin d'éviter la propagation des données, où un scandale grave lié aux données personnelles – alors que l'affaire Cambridge Analytica, concernant aussi Facebook retentit en ce moment dans les médias[7]. L'avertissement doit être transmis à la CNIL, ou tout autre autorité compétente dans le pays en question, « dans les meilleurs délais », soit si possible 3 jours après en avoir pris connaissance, précise le Règlement ; si elle est effectuée plus de 3 jours après, il sera nécessaire de préciser les motifs de retard.

Une violation de données – synonyme de faille de sécurité – est une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. Notons qu'une faille de sécurité découverte sur un environnement précisément destiné à cela n'a pas à être signalée, ni celles qui n'ont révélé aucune donnée personnelle, il faut en effet une violation de données à caractère personnel, même si elle est minime, et surtout si vous n'êtes pas sûr de son ampleur.

La CNIL est là pour vous aider dans ce cas et jouera en premier lieu le rôle du pompier : éteindre le feu avant qu'il ne prenne trop. Au niveau pénal[8], la non-communication à la CNIL sera suivie de 5 ans d'emprisonnement et de 300 000 €, un paradoxe, quand on sait que la connaissance de cette faille par la CNIL peut mener à des amendes disciplinaires…

En cas de communication à la CNIL (c'est à ne pas souhaiter), il vous faudra fournir les éléments suivants, que la CNIL gardera bien évidemment privés[9] :

2. L. n° 78-17, 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, art. 34
3. RGPD, art. 5
4. ANSSI (ex-DCSSI), 2004, guide pour l'élaboration d'une politique de sécurité de système d'information
5. Par exemple le PSSI de l'État

— une description de la nature des données (quelles données ?) ainsi que, s'ils sont connus, les types de personnes touchés par la faille, et leur nombre ; s'il est approximatif, ou estimé en interne, fournissez-le tout de même (quel quantité ?), enfin, quelle quantité d'enregistrements a été effectuée ?
— le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
— expliquer les conséquences possibles et probables de la violation de données ; pas besoin d'en faire des tonnes, mais soyez clairs et allez droit au but ;
— décrire les mesures proposées pour remédier à la violation de données, et les mesures pour en atténuer les effets négatifs.

Comme vous pouvez le voir, cela représente beaucoup d'informations en 72 heures, c'est pourquoi il est recommandé d'ajouter à votre PSSI une politique de gestion des incidents, qui formalise le processus à effectuer en cas de problème sur un serveur ou de faille de sécurité, qui inclus notamment l'obligation légale de déclaration à la CNIL des failles de sécurité dont nous venons de parler ; en cas de problème, vous serez ravis d'avoir ce protocole sous la main.

Enfin, dans certains cas très précis, il est nécessaire d'avertir l'utilisateur que ses données personnelles ont été volées. Cela concerne les cas où la communication de ces données présente un risque élevé pour les droits et libertés ; pour vous aider là-dessus, la CNIL a mis sur son site Internet des guides à destination des professionnels de différents secteurs pour faciliter la compréhension.

III.1.4. Le PIA : une analyse d'impact

Le **P**rivacy **I**mpact **A**ssessement est un processus qui assure que tout nouveau traitement mis en en œuvre ou toute modification d'un traitement existant sera réalisé conformément aux obligations légales diverses, particulièrement relativement à la sécurité, la confidentialité et la fin de vie des données (après les cycles d'archivage)[10].

Ce PIA est toujours recommandé, mais obligatoire uniquement dans les cas « susceptible[s] d'engendrer un risque élevé pour les droits et libertés des personnes ». Pour déterminer cela, il faut utiliser le Règlement, qui définit des obligations de manière formelle, la CNIL, et sa bibliothèque d'avis, et d'avis à venir, mais aussi une liste, mise en place par le G29 (deux éléments de la liste devraient vous alerter et vous inciter à réaliser un PIA) qui vous indique de vous inquiéter dans les cas[11] :

— d'évaluation et de notation, y compris le profilage (d'un salarié, par exemple) ;
— de prise de décision automatisée, dans un cadre juridique (c'est pourquoi la nouvelle loi de conciliation de justice impose un humain dans le processus, notamment) ;
— de surveillance systématique, sans que soit entendu par surveillance l'idée de caméra ;
— données particulières visées à l'article 9 (de santé, pénale, …) ;
— de big-data, important par sa volumétrie, le nombre de personnes concernées, la durée de conservation et l'étendue géographique du traitement ;
— de croisement d'informations entre elles ;

6. RGPD, art. 33 et suivants
7. Rappel succin des événements
8. C. pén., art. 226-17-1
9. RGPD, art. 33, alinéa 3

— de traitement de données de personnes vulnérables (pour rappel, mineur de 16 ans et majeurs protégés) ;
— de l'emploi de solutions technologiques particulièrement technologiques (entendre innovantes et dangereuses, comme la biométrie) ;
— enfin, d'exclusion du bénéfice d'un droit du RGPD (si l'utilisateur est privé de droit d'accès par exemple).

Comme je le disait plus haut, il faut deux points pour commencer à s'inquiéter suffisamment pour réaliser un PIA, mais si vous ne répondez qu'à un critère, soyez toutefois vigilant : vous traitez une donnée sensible, soumise à des règles parfois spécifiques. Prenons un exemple : le traitement de données de patients ; par un hôpital, un PIA devra être réalisé, car les conditions « personnes vulnérables », « données sensibles » et « big-data » – oui, pas au sens commun, on parle de big-data quand un bon nombre de personnes sont concernées. Par un médecin, toutefois, pas besoin de PIA, car les médecins bénéficient d'une exception au sens du considérant 91 du RGPD.

Pour bien rédiger un PIA, je vous redirige vers les très bons conseils de la CNIL à ce sujet, car sa documentation est plus complète que n'importe quel cours.

Terminons enfin par préciser qu'il faut transmettre le PIA à la CNIL s'il réside un risque élevé malgré la mise en place de protocoles pour l'éviter, sur obligation légale ou en cas de contrôle de la CNIL dans l'entreprise ; il est en tous cas conseillé de refaire un PIA au moins tout les 3 ans, ou au moins de le revoir, cela permets de se rendre compte des données devenues inutiles, et des informations devenues inexactes.

J'espère que ces concepts de confidentialité et de sécurité sans bien ancrés dans vos têtes, et que vous y penserez lors de la réalisation d'un quelconque projet informatique. Pour rappel la question importante à se poser est la suivante : « La sécurité des données que je traite est-elle proportionnée à leur contenu ? ».

10. RGPD, art. 35
11. G29, avis WP 248, lignes directrices concernant l'analyse d'impact relative à la protection des données, 4 avril 2017

III.2. Le transfert des données hors de l'UE

Ici, nous traiterons du transfert des données de citoyens européens en dehors de l'Union, soumis à des règles d'exception : le principe général est la demande de consentement, mais nous verrons que ce principe pose de nombreux problèmes et est très contraignant, c'est pourquoi le législateur met en place de nombreuses dérogations, afin d'ajouter de la souplesse à ce système de consentement explicite, qui ne subsiste que pour les données sensibles.

III.2.1. Présentation et principes généraux

La donnée est aujourd'hui devenue vitale pour l'économie et la société, et de nombreuses dynamiques se mettent en place autour, dont des échanges de plus en plus internationalisés. Avant le RGPD, l'Europe ne protégeait pas les données circulant hors de son sol, mais comme nous l'avons vu, le champ d'application du Règlement dont ce cours est l'objet a été élargi pour englober les données concernant tout citoyen européen ; il est alors devenu indispensable pour le législateur d'encadrer les règles de sortie de données de l'UE, et de leur traitement à l'étranger.

Par principe, l'accord de l'utilisateur est nécessaire avant transfert de données personnelles hors de l'Europe, et ce pour la plupart des pays de l'Union ; certains pays, cependant, ont été jugés aptes par la Commission Européenne à prendre un soin suffisamment correct des données[1], ce qui leur permet de bénéficier d'un statut privilégié :

- l'Espace Économique Européen (c'est-à-dire l'UE plus Islande, Norvège et Liechtenstein), où la plupart des règles applicables en Union Européenne s'appliquent ;
- la Suisse, qui a une situation complexe en cela que l'accord sur l'EEE n'a pas été approuvé par référendum là-bas, ils n'en sont donc pas membres officiellement (mais bien conformes pour le RGPD) ;
- la Nouvelle-Zélande, le Canada, l'Argentine et Israël, qui ont des législations positives et sont donc reconnus adéquats ;
- les États-Unis, sans certitude, par le Privacy Shield, un accord qui devait permettre le libre-échange des données entre l'Europe et ce pays, mais qui est pour le moment au point mort, et pas encore appliqué.

Ces pays, donc (sauf pour le dernier), sont dits « adéquats », ou parfois « conformes », ce qui signifie qu'aucun consentement autre que celui nécessaire pour le recueil des données n'est requis auprès de l'utilisateur ; c'est un soulagement pour les entreprises, même s'il l'est peut-être moins pour les utilisateurs soucieux de leurs données, car ils devront passer par diverses structures.

Notons que le transfert doit toutefois faire l'objet d'une communication à l'utilisateur lors de l'exercice de son droit d'information ou de son droit d'accès[2] : il est nécessaire de préciser si le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers et d'informer l'utilisateur de l'existence ou de l'absence d'une

décision d'adéquation rendue par la Commission ou de toute autre mesure visant à assurer l'exercice de ses droits (les mesures dont nous parlerons juste après.

Enfin, sachez qu'une organisation internationale (type ONG), est considérée comme un pays étranger[3] pour le transfert de donnée, sauf s'il peut s'établir sur un État précis, et s'il souhaite s'établir sur cet État ; c'est recommandé, sauf en cas de besoin réel de mobilité de la donnée pour une ONG.

Le consentement est une méthode simple, mais celui-ci doit être libre, informé, spécifique et non ambigu, comme nous l'avons déjà vu ; cela le rend très complexe à mettre en place, et il faudrait développer une infrastructure parallèle en cas de refus, dans le pays concerné, ce qui semble tout de même très improbable, surtout pour les sociétés dont le business repose intégralement sur la donnée ; en pratique, il est surtout applicable pour les données sensibles, et des dérogations sont utilisées lors des transferts vers les pays non-adéquats.

III.2.2. Les règles spécifiques applicables

Avant toute chose, il me semble nécessaire de mentionner que des exceptions au consentement sont possibles, hors cas mentionnés ci-avant et ci-après, lors de motifs spécifiques et bien définis, que nous avons déjà vus dans une partie précédente, et que je rappelle ici ; les données personnelles d'un utilisateur peuvent être transférées, sans son accord, lorsqu'icelui[4] :

- est nécessaire à l'exécution d'un contrat auquel la personne concernée a souscrit, seulement lors de nécessité absolue du traitement ;
- est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ;
- est nécessaire à l'exécution d'une mission d'intérêt public, sans précisions sur la notion de « mission d'intérêt public » ;
- est nécessaire pour l'exercice de la justice dans le pays concerné, par exemple, le transfert peut être effectué vers un autre pays, depuis la France, si ces données sont nécessaires à la justice là-bas ;
- enfin, si les données sont publiques.

Hors de ces exceptions notables, dont on remarque qu'elles sont moins nombreuses qu'à l'accoutumée ; le principe du RGPD concernant le transfert des données en dehors de l'Union n'est pas d'interdire, mais simplement de règlementer, pour créer un cadre à la fois propice aux utilisateurs, mais aussi en entreprise, en leur simplifiant au maximum le travail. C'est la raison d'être des différents accords que nous verrons ici : ils ne visent pas à empêcher les entreprises de transférer leurs données, mais simplement de les contraindre à le faire dans les règles.

La première possibilité de déroger au consentement sont les accords juridiques spécifiques en États ; nous en parlions juste avant, cela ne concerne pour le moment que le Privacy Shield[5], appelé auparavant Safe Harbor, qui vise à une « harmonisation » des règles entre les Etats-Unis et l'Europe sur la protection des données. Cet accord prévoit que la juridiction états-unienne prévaut en cas de conflit, même si son droit n'est pas seul applicable aux données – un droit spécifique s'applique pour le traitement des données, et est précisé dans l'accord. Ce Privacy Shield est très complexe, et il pourrait faire l'objet d'un cours entier, sachez en tout cas qu'il est

1. RGPD, considérant 104
2. RGPD, art. 13
3. RGPD, art. 44

pour le moment délicat de l'appliquer, car il est très critiqué, et il semble évident qu'il va être supprimé prochainement.

Un moyen plus simple d'éviter le consentement sont les « Model Contracts », ou Clauses Contractuelles Types en français ; ces clauses sont en fait des modèles non-modifiables de conditions régissant le transfert des données. En particulier, ces clauses prévoient que la loi européenne doit être applicable avant et pendant le transfert, et continue de l'être après si elles concernent un citoyen européen, qui peut exercer ses droits auprès de l'organisme local qui a collecté ses données. Ces clauses sont en pratique assez utilisées, car elles existent depuis longtemps ; elles sont simples mais peu flexibles, car il n'en existe que deux types (2001 et 2004), et la seule partie modifiable sont deux annexes (définition et mesures de sécurité) ; notons de plus que ce moyen est l'objet d'un recours actuellement, il est donc « à risque ».

Un second moyen important[6], qui est sûrement le plus important mis en place par le RGPD, sont les BCR – ou Règles d'Entreprise Contraignantes, qui consistent en la mise en place d'une gouvernance globale des données au sein d'une structure. Ces règles sont juridiquement contraignantes, et confèrent certains droits obligatoires aux utilisateurs. C'est une solution flexible, aisée pour une société moyenne mais peu accessible aux petites entreprises, de par leur complexité juridique. *A minima*, ces règles doivent contenir[7] :

— les finalités du traitement ;
— les personnes affectées par le transfert, car il ne concerne pas forcément toutes les personnes dont les données sont traitées ;
— les pays destinataires ;
— une mention de leur nature juridiquement contraignante ainsi que la mise en place des principes fondamentaux de la gouvernance des données dans l'entreprise ;
— les divers mécanismes de réclamation et d'exercice des droits pour les utilisateurs ; ces droits devront leur être mentionnés ailleurs, car les BCE sont des documents internes ;
— les mécanismes internes et procédures d'audit mises en place pour assurer les données et leur bon traitement, ainsi que les mesures de formation du personnel mis en place pour les atteindre.

Ces règles me semblent une très bonne solution dans le cas d'une grande quantité de données ; notez en tout cas qu'elles ne sont pas juste une formalité administrative, mais visent à remettre en cause **en profondeur** la façon dont les données sont gérées, car seule une réforme interne à l'échelle de l'entreprise permet leur bonne application.

Terminons par mentionner deux possibilités, qui, au moment au j'écris ces lignes, ne sont pas encore ouvertes : les codes de conduite, qui sont des procédures internes à une entreprise et approuvées de façon globale par la Commission Européenne ou un État membre, ainsi que les certifications, attribuées aux structures respectant certaines règles de bonne conduite, et pouvant donner lieu à une autorisation de transfert. Ces deux modes d'actions sont encore mal définis[8], car la Commission y travaille toujours, conjointement avec le G29.

Pour terminer, je vous propose dans la partie suivante un petit résumé de ce que nous avons vu jusqu'à maintenant, avec une carte de transfert des données, et un rappel des diverses possibilités

de se passer du consentement.

III.2.3. Un schéma-bilan des pays

La CNIL propose sur son site une carte interactive sur les divers modèles à adopter pour transférer de la donnée en fonction des pays du monde ; je propose ici une carte d'ensemble, plus simple (et donc moins spécifique) que celle de la CNIL, qui est surtout à vocation indicative.

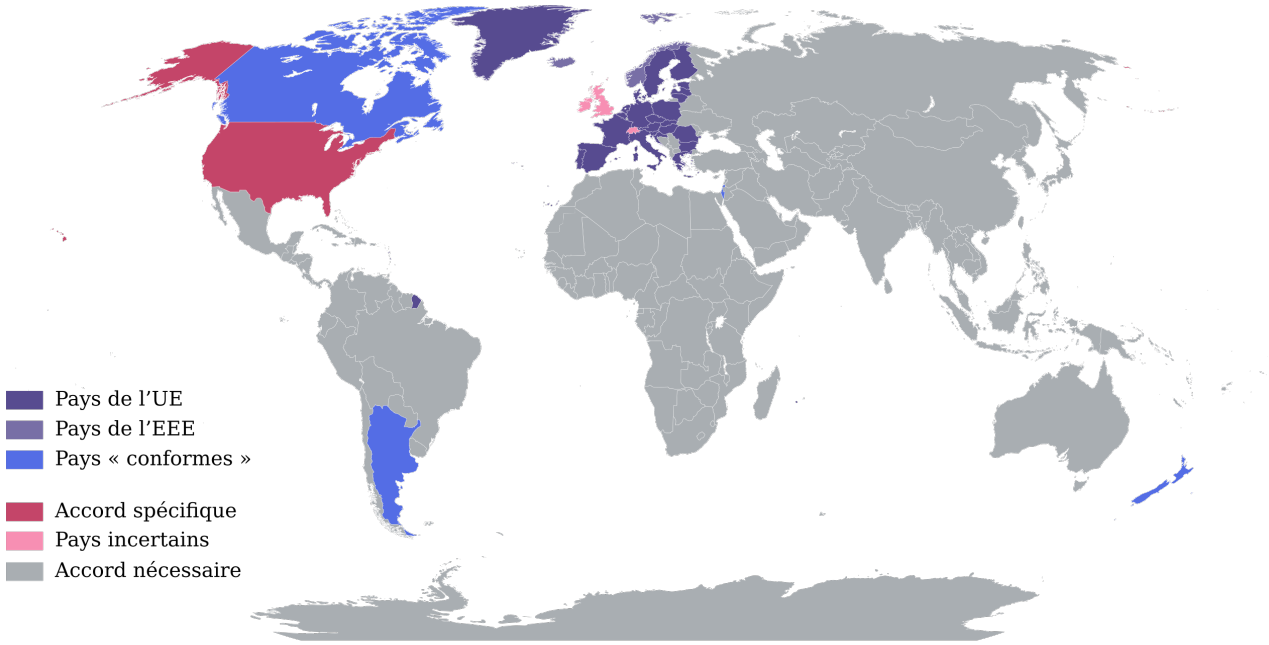

FIGURE III.2.1. – Carte de conformité RGPD

Pour les pays incertains, j'ai inclus le Royaume-Uni et l'Irlande, car on ne sait pas ce qu'il adviendra au niveau de la sortie de l'UE, ainsi que la Suisse pour sa situation particulière. Pour le reste, la carte semble grise, mais il faut noter que nombreux pays grisés ne seront même jamais l'objet d'un de vos transferts internationaux.

Pour les pays où un accord est nécessaire, il peut prendre la forme, pour rappel :

- d'un consentement ;
- d'une exception légale au consentement ;
- du transfert vers un pays « adéquat » ;
- d'un accord inter-États ;
- de « Model Contract », si les données à transférer sont simples ;
- de BCR, pour les grandes et moyennes entreprises, lorsque la volumétrie est importante ou que les données sont particulièrement sensibles.

4. RGPD, art. 49
5. Voir le site officiel
6. RGPD, art. 47
7. RGPD, art. 47, alinéa 2
8. RGPD, art. 40 et suivants

En cas de questionnement sur le transfert de vos données, je vous invite à revenir à cette carte et à compléter éventuellement votre recherche par la carte proposée par la CNIL. Si vous adorez le RGPD, cette carte est distribuée sous licence libre, vous pouvez donc même l'accrocher au mur de votre chambre.

III.3. La gestion des données sensibles

Je le mentionnais au début du cours, certaines données sont considérées sensibles, et sont directement listées par le texte du Règlement. Ces données, de par leur caractère sensible, sont bien évidemment à protéger avec beaucoup de soin, et nous verrons en quoi cela impose des mesures accrues en termes de protection, sécurité et confidentialité.

III.3.1. Qu'est-ce qu'une donnée sensible et cas général

Avant tout traitement de donnes, il est nécessaire de vérifier si les données à traiter ne sont pas considérées sensibles ; c'est un cas très particulier, car le Règlement permet de traiter n'importe quelle donnée. Pour éviter les abus, le RGPD établi directement[1] la liste des données à caractère sensible, mais elle peut être complétée par les États selon leurs propres règles internes. Trois cas sont à ne pas confondre lors du traitement de données : les données à caractère sensible, les données d'infraction, et le numéro de sécurité sociale.

Pour le premier cas, concernant les données sensibles, icelles doivent relever d'un des champs suivants pour que les règles mentionnées ci-après s'appliquent :

- l'origine raciale ou ethnique ;
- les opinions politiques ou l'appartenance syndicale ;
- les convictions religieuses ou philosophiques ;
- le traitement des données génétiques, y compris des données biométriques aux fins d'identifier une personne ;
- les données concernant la santé ;
- les données concernant la vie sexuelle ou l'orientation sexuelle.

La collecte de ces données est interdite en toutes circonstances, sauf quelques rares exceptions que nous verrons ci-après, il faut en tout cas être extrêmement vigilant lors de la collecte de ces données ; tout traitement de données sensibles devrait immédiatement alerter le responsable du traitement ou l'utilisateur dont les données ont été traitées, car une vérification légale s'impose alors.

Concernant les données d'infraction, elles ne font l'objet d'aucune des exceptions[2] que nous verrons plus bas ; ces données ne peuvent être traitées que sous contrôle de l'autorité publique. En particulier, tout registre complet de condamnation ne peut être tenu que sous le **contrôle** de l'autorité publique – notez ce mot de contrôle, qui précise que le traitement peut être effectué par un organisme privé, tant qu'il agit sous la subordination directe de l'autorité publique, c'est la fameuse sous-traitance dont nous parlions plus tôt, appliquée aux administrations. Les données de suspicion sont soumises aux mêmes règles de traitement, et donc limitées aux cas de nécessité de l'autorité publique.

Enfin, le numéro de sécurité sociale n'est pas considéré par le RGPD comme une donnée sensible, mais il l'est au niveau de la loi française actuellement, et comme il est possible pour les législateurs nationaux d'ajouter certains types de données sensibles, il est probable que cette loi reste – rappelez-vous du projet SAFARI, qui avait fait scandale à l'époque ; il faudra donc surveiller les transpositions des différents pays, ainsi que la jurisprudence de la CJUE à ce sujet.

III.3.2. Des exceptions rares

Les données à caractère sensible peuvent toutefois être traitées dans certains cas d'exceptions, lorsqu'une loi particulière le permet, elles peuvent alors être traitées avec les précautions que nous verrons ci-dessous. Par exemple, les données sensibles relatives aux employés peuvent dans certains cas être stockées par l'employeur lorsque la convention collective le permet[3] ; aussi, des dispositions spécifiques s'appliquent aux banques et assurances concernant les données de leurs clients[4].

Par ailleurs, une liste est prévue par le RGPD pour autoriser dans certains cas le traitement de données sensibles, lorsque aucune loi particulière ne le permet, dans les cas suivants[5] :

— lorsque la personne concernée a donné son consentement explicite, un cas qui revient souvent dans le RGPD comme vous avez sûrement pu le remarquer : tout peut être traité sous réserve de consentement explicite ; dans ce cas, le consentement doit comme toujours être éclairé, ce qui signifie que vous devez préciser à l'utilisateur que vous traitez des données sensibles ;
— le traitement est strictement nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne visée par le traitement n'est pas apte à donner son consentement ; encore une fois, nous avons déjà traité ce cas, avec l'exemple de l'hospitalisation en urgence ;
— si le traitement de données concernant les opinions politiques, l'appartenance syndicale, les convictions religieuses ou philosophiques est effectué par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, pour la liste exclusive de ses membres, sous réserve de garanties appropriées et sans que le fichier soit diffusé ;
— lorsque les données sont manifestement publiques, ou ont été rendues publiques par la personne concernée ;
— le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'UE ou de dispositions spécifiques d'un État membre, sous réserve de proportionnalité entre l'objectif poursuivi et le respect des droits fondamentaux ; on parle ici du droit particulier du renseignement, qui doit tout de même prévoir des garanties de respect des droits des personnes ;
— les données de santé sont traitées par un professionnel de la santé soumis au secret médical ou « lorsque le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de

1. RGPD, art. 9
2. RGPD, art. 10

sécurité des soins de santé et des médicaments ou des dispositifs médicaux », sous réserve de dispositions de l'UE ou d'un État membre ;
— à des fins statistiques, historiques ou archivistiques, sous réserve de respecter le droit des personnes.

Concernant les données d'infraction, je mentionnais ci-dessus qu'aucune des exceptions n'y était applicable, mais le législateur en prévoit tout de même une, bien différente, qui concerne le traitement de données pour son propre contentieux[6] ; on pourrait citer deux exemples, celui de l'entreprise impliquée dans des affaires judiciaires et ayant besoin de stocker les données relatives au contentieux, tant les informations concernant son entreprise que celles concernant la partie adverse.

III.3.3. En cas de traitement : des procédures renforcées

III.3.3.1. Informations à l'utilisateur et hygiène numérique

Le Règlement précise que lorsque le traitement est fondé sur base de données sensibles, il est nécessaire d'informer l'utilisateur de son droit à retirer son consentement[7] (règle générale) en même temps qu'il est informé de tout les points que nous avons mentionnés dans l'obligation de transparence. Ce droit doit lui être rappelle lorsqu'il en fait demande, et il doit absolument être applicable, c'est-à-dire que si le traitement n'est fondé que sur le consentement de l'utilisateur, et qu'il retire son consentement, le traitement doit alors cesser[8].

En cas d'autres dispositions (ou exceptions) qui autorisent le traitement, il est en tout cas nécessaire de considérer le retrait du consentement de la personne concernée, particulièrement en ce qui concerne le transfert des données à d'autres entités, qui peut se retrouver interrompu, ou simplement rompu, car la sensibilité des données doit particulièrement être prise en compte lors du transfert des données, que ce soit hors UE ou à une organisation externe située dans l'Union.

Aussi, il sera nécessaire d'effectuer une formation du personnel afin de le sensibiliser à ces problématiques, en considérant les mesures à mettre en place à leur niveau, sous la supervision particulière du DPD, qui doit en tout cas jouer un rôle majeur dans la détermination du droit de traitement de ces données sensibles, ainsi que dans la mise en place de processus de démonstration de la conformité.

III.3.3.2. Sécurité et confidentialité

Au niveau de la confidentialité, elle doit nécessairement être renforcée, et comme nous le mentionnons ci-avant, tout passage par un sous-traitant, transmission à une entreprise externe ou transfert dans un pays non-conforme devra être scrupuleusement vérifié : il faudra ainsi adjoindre à vos BCR des dispositions à ce sujet ; notons enfin que les « Models Contracts »

3. RGPD, art. 9, alinéa 2.b
4. Voir la page thématique de la CNIL
5. RGPD, art. 9, alinéa 2
6. RGPD, art. 10

dont nous parlions à la partie précédente ne sont pas applicables dans le cas de données sensibles, une gouvernance des données concernant toute l'entreprise devra alors être mise en place.

Comme je le mentionnais ci-avant, le traitement de données à caractère sensible est l'un des cas où le recours à un DPD est obligatoire[9] au niveau du RGPD (cela vaut donc dans tout les pays européens). Le DPD doit donc assurer, de part ses connaissances nécessaires au sécurité informatique, que toute les mesures nécessaires sont mises en œuvre pour protéger les données des personnes.

Cela passe en particulier par une pseudonymisation des données sensibles, et leur répartition sur plusieurs bases de données et serveurs différents, afin d'éviter les fuites totales permettant l'identification des personnes en cas de vol de données. Une autre mesure technique importante à mettre en place lors du traitement de données sensibles est le chiffrement, si possible de bout-en-bout lors des communications, et éventuellement un chiffrement complet sur le serveur, ce qui évite les fuites dangereuses pour les utilisateurs.

Le point important de cette partie est de vous amener à toujours vous demander si certaines données que vous traitez, ou serez amenés à traiter, sont dites sensibles au niveau du Règlement ; il faut pour cela vous référer à une interprétation stricte de la liste fournie. Après avoir déterminé si vous traitez des données sensibles, n'oubliez pas de vous demander si vous en avez le droit, en déterminant l'exception applicable.

Ce cours sur le RGPD est quasiment terminé, il ne nous reste qu'à traiter la partie du rôle de la nouvelle CNIL, qui sera très différente de l'ancienne en cela que ses missions de contrôle seront plus *a posteriori*, directement en entreprise, qu'*a priori*, comme avant, par le biais de déclarations.

7. RGPD, art. 13, alinéa 2.c
8. RGPD, art. 17, alinéa 1.b
9. RGPD, art. 37, alinéa 1.c

Quatrième partie

Rôles de la CNIL

Pour terminer ce tutoriel, nous allons étudier deux aspects différents d'une même instance : la **C**ommission **N**ationale **I**nformatique et **L**ibertés, qui est française, mais doit nécessairement avoir un équivalent dans chaque pays où le RGPD est en vigueur. Cette commission existait déjà, mais elle va devoir faire peau neuve et adapter ses méthodes de travail pour être conforme à la nouvelle réglementation.

IV.1. Le renouveau de la CNIL

IV.1.1. Allègement de la CNIL, renforcement du G29

Nous l'avons vu, avec le RGPD, la CNIL n'est plus un acteur central du contrôle des données personnelles ; c'est maintenant l'entreprise qui gère toute sa conformité de A à Z sous la supervision d'un DPD. Pour ces raisons, la CNIL a choisi de s'effacer de plus en plus au profit du G29, qui regroupe toutes les CNIL européennes, l'objectif étant bien évidemment une concordance des décisions européennes dans le cadre d'une concordance des lois européennes.

Un nouveau système de guichet unique est en cours de mise en œuvre et permet aux entreprises, ainsi qu'à la CNIL, de ne s'adresser qu'à un seul acteur concernant les données qu'elles traitent dans toute l'Union. Ce système pose la notion d'établissement principal, qui est généralement l'établissement où se situe le siège social de l'entreprise, mais il peut concerner une filiale qui aurait une indépendance complète quant au traitement de données. Cet établissement principal est très important au niveau du RGPD, car il définit l'autorité de contrôle avec laquelle l'entreprise aura à traiter lors de ses demandes, mais aussi des divers contrôles qui seront effectués.

Au titre de ce principe de guichet unique, l'autorité locale de contrôle conserve toutefois des droits de sanction, mais aussi de nombreux rôles qui ne sont pas transférés à l'Europe ; la CNIL conserve en premier lieu son rôle de conseil, auprès des entreprises, mais aussi des autorités publiques et du grand public ; en effet, il est nécessaire de fournir à l'ensemble des acteurs des outils et des référentiels afin qu'ils puissent facilement se mettre en conformité avec le nouveau Règlement ; par exemple, elle met en ligne sur son site un petit programme à télécharger permettant d'effectuer facilement des analyses d'impact.

Ensuite, la CNIL à un rôle en amont, qui consiste à suivre l'évolution des technologies et à réfléchir sur les nouvelles problématiques éthiques qui pourraient être mises en œuvre ; à cet effet, elle mets en place un laboratoire des nouvelles technologies pour étudier les nouveautés, et lance parfois des débats publics pour prendre en compte l'avis du plus grand nombre de personnes, comme son débat sur les algorithmes, dont les réponses ont été publiées le 06 juin 2017.

IV.1.2. Diminution des procédures obligatoires...

Alors qu'auparavant, les procédures auprès de la CNIL étaient obligatoires, préalablement à tout traitement de données (hors exceptions de la loi ancienne), le principe d'« accountability » lui restreint énormément son champ d'action. Il y a tout de même deux situations où la CNIL reste maître du jeu : celles dans lesquelles le règlement prévoit effectivement des autorisations que devra donner la CNIL, c'est le cas pour les autorisations de transfert, hors procédures

dérogatoires, ou lorsque ce seront des arrangements administratifs entre autorités publiques qui n'auront pas de valeur contraignante (oui, c'est possible).

La deuxième possibilité, qui reste une grosse inconnue pour le moment, ce sont les marges de manœuvre laissées aux États, qui pourront rajouter des dispositions dans leurs lois nationales (en France, la loi de 1978). Ces marges de manœuvre sont toutefois limitées à certains domaines, comme le traitement des données de santé ou des données génétiques, données biométriques ou l'utilisation du numéro de sécurité sociale.

Hormis ces deux cas, qui comme nous l'avons vu ne sont pas clairement définis, les entreprises ne sont plus tenues dans les autres domaines de contacter l'autorité de contrôle, tout se passe en interne, même si le recours *a priori* à la CNIL reste autorisé, et même fortement conseillé dans certains cas où le doute subsiste ; la structure fait alors appel, par l'intermédiaire de son DPD, à la CNIL afin de la conseiller dans la mise en œuvre d'un traitement.

IV.1.3. …remplacées par de nouveaux contrôles

D'un autre côté, la CNIL gagne de nombreux pouvoirs de sanctions, qui seront donc appliqués *a posteriori* ; ces pouvoirs sont maintenant très importants, à commencer par la possibilité de contrôle des registres de traitement, des diverses analyses d'impact, des PSSI, et autres dispositifs de preuve – de fond ou de forme, de la conformité.

En plus de cette possibilité de contrôle, la CNIL se voit dotée d'un pouvoir de sanction bien plus important qu'avant, pour deux raisons : tout d'abord, il s'applique hors de l'Union Européenne (extraterritorialité), et concerne ainsi bien plus de traitements et d'entreprises. La seconde raison est le renforcement des sanctions administratives pouvant être prononcées : jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise ou 150 000 €, le montant le plus élevé étant retenu.

On entre aujourd'hui dans une nouvelle phase où la protection des données doit vraiment être prise au sérieux ; pour autant, la CNIL devrait modérer ses sanctions, particulièrement au niveau des entreprises n'ayant pas eu le temps de se mettre en conformité, le plus important étant de montrer des signes de tentatives actives de protection des données, pas tant d'être immédiatement en conformité. Il y a toutefois fort à parier que les entreprises qui se fichaient hier des sanctions de la CNIL, et n'écoutaient pas ses avertissements, seront punies rapidement et d'un montant dissuasif ; il y a donc effectivement un nouveau mode de politique de sanction, vers lequel l'Europe veut tendre.

IV.2. Les formes et principes de recours

Dans cette section, nous allons voir comment, en tant que personne, il est possible de s'opposer à une utilisation illégale de ses données.

IV.2.1. Le recours gracieux

La première méthode de recours est appelée recours gracieux, et consiste en fait à s'adresse d'abord à l'entreprise concernée et effectuant le traitement de données ; ce recours est utile particulièrement dans les cas où certaines informations quant à l'application du RGPD ne sont pas précisées sur le site, comme les coordonnées du responsable de traitement, ou lorsqu'une fonctionnalité nécessaire est inexistante ou inutilisable, par exemple, si l'on ne peut pas supprimer ses informations personnelles d'un site.

Ce recours est déconseillé dans les cas où une réponse négative vous a déjà été apportée par un traitement humain, c'est-à-dire dans les cas où une personne physique, et non un algorithme, vous a refusé, pour des motifs légitimes ou non, l'application d'un droit du RGPD. Quelques exceptions sont à marquer toutefois, comme le cas du recours hiérarchique, qui est un cas particulier du recours gracieux, et qui consiste à réitérer une demande, ou à contester un refus face au supérieur hiérarchique de la personne ayant pris la décision.

Le recours hiérarchique est d'utilité moindre dans le cas du RGPD, mais si un employé de l'entreprise vous refuse l'exécution d'un droit, vous pouvez toujours tenter de contacter le responsable du traitement pour l'informer du problème, ou éventuellement contacter le DPD si la situation est grave, afin qu'il remette l'entreprise sur les bons rails. Ce droit peut aussi être utilisé dans le cadre du travail, si vous souhaitez obtenir des informations sur vos données, vous pouvez tenter de contacter le patron, ou un supérieur pour éviter d'envenimer la situation en faisant appel à la CNIL.

Hors procédures de recours, il est bien entendu nécessaire de tenter les voies prévues par le service pour faire respecter ses droits, avant d'envoyer toute plainte à la CNIL – par exemple, inutile d'envoyer une plainte si vous n'avez jamais tenté d'envoyer un courrier avant : il faut faire preuve de bonne volonté. Pour vous aider à rédiger vos courriers à destination des différents acteurs du traitement, la CNIL propose un catalogue de modèles sur son site Internet.

IV.2.2. Le recours à la CNIL

Lorsqu'une infraction au RGPD est dûment constatée par un utilisateur, il est recommandé d'avertir la CNIL, et cela même si vous n'êtes pas entièrement sûr qu'un droit a été bafoué – évitez toutefois les plaintes farfelues, évidemment non-fondées ou diffamatoires, vous pourriez

avoir des ennuis, en plus d'en avoir causé à la CNIL… Pour adresser une plainte légitime, vous pouvez passer soit par un formulaire en ligne , soit par courrier postal à l'adresse :

Suite à cette plainte, la CNIL jugera s'il est nécessaire ou non d'effectuer des contrôles dans la structure concernée, puis vérifiera votre plainte et, en fonction de la gravité, la commission pourra prononcer, selon les cas :

— une mise en demeure (avertissement), qui est en quelque sorte un premier avertissement : l'entreprise concernée devra s'y conformer dans un délai imparti ; cette sanction est prononcée par le président de la CNIL, après une procédure contradictoire et la sanction peut être rendue publique afin de faire de la mauvaise publicité à la structure ou non ;
— une sanction pécuniaire (sauf pour les traitements effectués par l'État) jusqu'à 4 % du chiffre d'affaires de l'entreprise, qui est aussi prononcée à l'issue d'une procédure contradictoire, et peut être contestée devant le Conseil d'État ;
— une injonction de cesser le traitement, c'est-à-dire une interdiction temporaire ou définitive de traiter un certain type de données ;
— le retrait d'un label ou d'une certification obtenue par la structure concernée.

En tout cas, l'autorité de contrôle auprès de laquelle la réclamation a été introduite est tenue d'informer l'auteur de la réclamation de l'état d'avancement et de l'issue éventuelle de sa réclamation ; aussi, elle doit l'informer de la possibilité d'un recours juridictionnel, que nous verrons juste après.

IV.2.3. Le recours juridictionnel

Pour terminer, parlons rapidement du droit au recours effectif devant la juridiction compétente, qui vous permet, si vous êtes sûrs de la violation du Règlement, d'assigner en justice l'entreprise ayant réalisé le traitement (ou l'État, dans une juridiction administrative). Cette procédure est contradictoire, et peut mener à des frais importants, contrairement au recours auprès de la CNIL : des frais d'avocats peuvent être nécessaires, et la partie adverse, si elle gagne, peut vous demander un remboursement des frais du procès, je vous conseille donc de bien vérifier la loi et de faire preuve de prudence lors du recours à la justice.

Un deuxième type courant de recours juridictionnel est la plainte déposée contre une autorité de contrôle, par une entreprise ou un particulier, qui ont droit au recours face à une décision juridiquement contraignante uniquement – et pour les mises en demeures. Ce recours peut aussi être déposé, dans les deux mois, face à une autorité de contrôle ne donnant aucune nouvelle quant à l'avancement du recours, elle doit par contre être effectuée devant la cour compétente dans le pays dans lequel se situe l'autorité de contrôle ayant rendu la décision litigieuse.

Une courte partie, comme vous avez pu le constater, qui réponds quelque part pour les entreprises à la question « Quels sont les risques ? », et pour les utilisateurs à la question « Comment exercer mes droits ? » ; deux questions importantes, qui pourraient être approfondies par la consultation directe du Règlement.

Vous êtes maintenant parés pour vous mettre en conformité avec ce nouveau Règlement, protecteur des utilisateurs et mis en place suite au laxisme de certaines entreprises quand au respect de la confidentialité des données personnelles de certains utilisateurs, ou suite au refus de suppression de données dans certains cas. Il permet en tout cas d'harmoniser le cadre au niveau européen et national, car toute multinationale traite des données de citoyens européens.

Mes remerciements à Dwayn pour ses relectures attentives durant la bêta, à Arius d'avoir partagé son expertise en matière de droit et à qwerty pour sa validation soucieuse du détail.

Liste des abréviations

CJUE Cour de Justice de l'Union Européenne. 29, 30, 44

CNIL Commission Nationale Informatique et Libertés. 2, 5–7, 9, 11, 15, 20, 22, 28, 29, 34–37, 41, 42, 45–53

PIA Privacy Impact Assessement. 2, 12, 36, 37

PSSI Politique de Sécurité des Systèmes d'Information. 12, 34–36, 50