Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES

TELEDOC 792
BATIMENT NECKER
120, RUE DE BERCY
75572 PARIS CEDEX 12

N° 2018/01/CGE/SG/TS

Avril 2019

Le Règlement général sur la protection des données : quelles opportunités pour les entreprises françaises ?

Rapport à

Luc Rousseau
Vice-président du CGE

établi par

Benoit LEGAIT
Ingénieur général des Mines

Rémi STEINER
Ingénieur général des Mines

Robert PICARD
Ingénieur général des Mines

Philippe LOUVIAU
Ingénieur général des Mines

Maurice SPORTICHE
Administrateur civil hors classe

Rémi LEFEBVRE
Assistant de mission

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

SOMMAIRE

SYNTHESE

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est reconnue comme un droit fondamental, tant par la Charte des droits fondamentaux de l'Union européenne que par le traité sur le fonctionnement de l'Union européenne. Depuis le 25 mai 2018, c'est un nouveau texte, le règlement général sur la protection des données personnelles (RGPD)[1], qui détermine les contours de cette protection.

Ce règlement, dont un considérant énonce que « *le traitement des données à caractère personnel devrait être conçu pour servir l'humanité* », se substitue à des règles précédemment définies sous la forme de directives. Il fallait en effet, selon la Commission européenne, surmonter l'insécurité juridique et les obstacles à une libre circulation des données qu'induisaient des différences de transposition entre les Etats membres.

Le RGPD se démarque des règles antérieurement applicables par deux évolutions principales : d'une part, il renforce les droits des ressortissants européens ; d'autre part, il remplace une obligation générale de notification *a priori* des traitements de données par une responsabilisation accrue des responsables de traitement, assortie d'un contrôle *a posteriori*.

Une étude menée en 2017 pour le compte de la Commission européenne[2] a permis d'estimer l'évolution, pays par pays, de plusieurs indicateurs économiques caractérisant le marché des données :

- le nombre des professionnels du traitement des données en France, estimé à 680 000 en 2014, à 705 000 en 2015 et à 740 000 en 2016, pourrait être compris entre 780 000 et 1 200 000 en 2020 ;
- le chiffre d'affaires agrégé des entreprises spécialisées dans le traitement des données, estimé en France à 8 milliards d'euros en 2016, en progression de 8 % par rapport à 2015, serait compris entre 10 et 12 milliards d'euros en 2020 ;
- plus globalement, l'ensemble des impacts directs et indirects sur l'économie du traitement de données, estimé à 38 milliards d'euros en France en 2016 (soit 1,51 % du PIB) et en hausse de 4,5 % par rapport à 2015, pourrait représenter entre 46 et 89 milliards d'euros en 2020 (soit entre 1,98 % et 3,39 % du PIB).

Quelques mois après la date d'entrée en vigueur du RGPD, le Conseil général de l'économie a estimé utile de recueillir et d'analyser l'expérience d'entreprises de tailles variées. En effet, si le RGPD vise à

---

[1] Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement Général sur la Protection des Données)

[2] *European Data Market, SMART 2013/0063, Final Report*, IDC and Open Evidence, 01/02/2017 http://datalandscape.eu/study-reports/european-data-market-study-final-report http://datalandscape.eu/european-data-market-monitoring-tool

Les prévisions sont établies dans trois scénarios, sous-tendus chacun par des jeux d'hypothèses portant à la fois sur les évolutions macro-économiques, l'essor des nouvelles technologies (internet des objets, « cloud », transformation numérique) et les initiatives publiques (en faveur notamment de formations spécialisées, de l'open-data et des standards ouverts). Les effets propres au Brexit, trop incertains, ne sont pas quantifiés.

assurer une meilleure protection aux données personnelles des citoyens, de nombreuses entreprises avaient exprimé des appréhensions à la perspective de son entrée en vigueur.

Il s'agissait pour le CGE de comprendre les interrogations suscitées par ce règlement et de formuler des recommandations pour que les entreprises tirent le meilleur profit du RGPD. Ces recommandations s'inscrivent dans plusieurs perspectives, qui sont autant de leviers d'action à court ou moyen terme :

- le partage d'informations et des meilleures pratiques, ainsi que **l'élaboration du droit souple** (« *soft law* ») à l'initiative des organisations professionnelles sectorielles et de la CNIL ;
- la mise en œuvre du mécanisme de **contrôle de la cohérence de l'application du RGPD au sein de l'Union européenne**, notamment à travers le rôle dévolu au Comité européen de la protection des données ;
- la contribution des pouvoirs publics français à la **préparation du rapport sur l'évaluation et le réexamen du RGPD**, que la Commission doit présenter au plus tard le 25 mai 2020 et tous les quatre ans par la suite au Parlement européen et au Conseil.

Le choix a été fait de focaliser l'examen à deux secteurs très réglementés et pour lesquels les données à caractère personnel peuvent présenter un caractère particulièrement intime : la santé et les services financiers[3].

Ces deux secteurs[4] employaient en 2016 dans l'Union européenne (Royaume-Uni inclus) un nombre comparable de professionnels du traitement des données : 618 000 pour la finance et 485 000 pour le secteur de la santé (sur un effectif total de 6 160 000). Mais la part que les professionnels du traitement des données représentent dans l'effectif total de ces secteurs d'activité est très différente : 9,4 % pour la finance et 2,0 % pour la santé, ce qui traduit leur maturité inégale à l'égard de l'exploitation des données et plus globalement en matière d'informatisation.

A cet égard, la valeur marchande des données échangées dans l'Union européenne en 2016, qui représenterait 11,8 milliards d'euros pour le secteur financier, est estimée à 1,8 milliards d'euros dans le secteur de la santé. Mais ce retard, qui tend à se résorber, pourrait aussi résulter pour partie de l'extrême sensibilité des données de santé. Du reste, la politique nationale sur le traitement de données massives fait une place privilégiée à ce secteur avec la mise en place d'un « Health Data Hub ».

Des auditions menées dans le cadre de cette mission ressortent plusieurs idées :

- Le RGPD est avant tout perçu comme une contrainte par les entreprises, une charge qui s'est avérée lourde et difficile à anticiper. Au sein des entreprises de petite taille, les moyens disponibles ne sont pas toujours à la hauteur de la complexité des enjeux et la qualité des offres de conseil exige une certaine circonspection[5]. Si les moyens humains et financiers dont

---

[3] Le caractère intime de ces données est évident dans le domaine de la santé ; les intitulés des opérations de paiement (cartes bancaires, virements SEPA…) peuvent également révéler beaucoup de détails sur la vie privée du titulaire d'un compte

[4] cf. étude *European Data Market*, note de bas de page n° 2

[5] cf. communiqué de la CNIL du 7 novembre 2018 : Pratiques abusives « Mise en conformité RGPD » : comment s'en prémunir avec la CNIL et la DGCCRF ?
https://www.cnil.fr/fr/pratiques-abusives-mise-en-conformite-RGPD-CNIL-DGCCRF

disposent les plus grandes entreprises sont plus conséquents, l'étendue de leurs travaux de mise en conformité l'est tout autant.

- La nouvelle logique de responsabilisation des acteurs, censée favoriser la prise d'initiative et l'innovation, engendre des craintes et des réticences, notamment en raison du montant élevé des sanctions potentielles. Les mises en demeure et les sanctions prononcées par la CNIL sont encore en nombre limité, mais nombreux sont ceux qui réclament des lignes directrices plus précises ou qui expriment le besoin d'être rassurés quant à la conformité de leurs traitements de données à caractère personnel.
- Les bénéfices potentiels du RGPD, résultant de son caractère moins prescriptif et d'une meilleure harmonisation européenne, sont occultés par un rapport coût/bénéfice immédiat peu profitable et par la rémanence de frontières nationales, induite notamment par des adaptations incomplètes et peu claires[6] du droit français. Sauf exception, les efforts fournis par les entreprises le sont à ce stade dans une perspective de conformité, et non de création de valeur ou de différenciation sur le marché.

Les principales difficultés auxquelles les entreprises ont été confrontées dans la perspective de l'entrée en vigueur du RGPD sont les suivantes :

- le **droit à l'effacement** est cité comme un des principaux chantiers : en effet, recenser la totalité des données liées à un individu **peut être difficile techniquement si les systèmes d'information n'ont pas été conçus à l'origine dans cette perspective**. Se pose aussi le problème consistant à discriminer les données personnelles qu'un client a souhaité effacer et les données que l'entreprise se doit de conserver en considération d'obligations extérieures au RGPD, par exemple de nature comptable, fiscale ou liées à la lutte contre la fraude. A cet égard, la puissance publique pourrait utilement favoriser l'émergence de solutions labellisées d'effacement ou d'anonymisation des données (**Recommandation 2**) ;
- le droit à la portabilité, qui est censé faciliter pour les consommateurs la décision de changer de prestataire de service, se heurte en pratique à la **nécessité de définir au préalable des cadres techniques d'interopérabilité** propres à chaque secteur professionnel, valables si possible à l'échelle européenne (**Recommandation 4**) ; faute de standards de restitution des données personnelles, le droit à la portabilité représente une charge importante pour les entreprises et un bénéfice incertain pour les consommateurs ;
- le recueil du consentement a constitué la manifestation la plus visible de l'entrée en vigueur du RGPD pour les consommateurs ; d'importants efforts ont été consentis par les entreprises, alors que **ces démarches, souvent formelles, conduisent en général le consommateur à des choix factices** ; en réalité, le RGPD n'impose pas le recueil du consentement lorsque l'entreprise a une obligation légale ou un intérêt légitime à traiter des données personnelles. Mais **il apparaît essentiel que les contours de l'intérêt légitime**

[6] Ces appréciations font référence à la promulgation de la loi du 20 juin 2018 plus de deux ans après la publication du RGPD et postérieurement à l'entrée en application de ce règlement ; au renvoi par cette loi à une ordonnance chargée d'apporter « *les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence* » de la loi n° 78-17 du 6 janvier 1978 ; à l'absence de publication à la date de rédaction du présent rapport du décret d'application de cette ordonnance du 12 décembre 2018 ; au choix de continuer facticement à se référer à la loi du 6 janvier 1978 plutôt qu'à un nouveau texte législatif venant au soutien du RGPD ; ou encore à l'articulation défaillante du droit européen et du droit national à l'égard des données de santé.

soient précisés par le droit souple et par le Comité européen des données personnelles (**Recommandation 6**), sans attendre que la jurisprudence vienne préciser cette notion ; c'est particulièrement le cas en ce qui concerne la question du traitement de données personnelles à des fins de Recherche et Développement, afin d'éviter qu'une mise en œuvre malavisée du RGPD ne freine l'innovation (**Recommandation 7**) ;

- le RGPD s'attache à lever les ambiguïtés qui peuvent exister entre la responsabilité des donneurs d'ordre et celle des sous-traitants, lorsqu'il est question de données personnelles ; de ce fait, l'ensemble des contrats de sous-traitance a dû être revu à l'occasion de l'entrée en vigueur du RGPD. Cette révision contractuelle a pu se révéler problématique, les sous-traitants étant évidemment enclins à engager une négociation plus large, notamment sur les prix, compte-tenu de leurs nouvelles responsabilités. **L'Etat doit lui-même revoir ses contrats avec le secteur économique** : le club des délégués ministériels à la protection des données (DPD) doit proposer une doctrine générale très rapidement (**Recommandation 9)** ;

- les entreprises qui collectent des données personnelles de personnes résidant sur le territoire européen doivent, sous le contrôle de la CNIL et sous peine de sanctions, mettre en œuvre des mesures de protection techniques et organisationnelles leur permettant d'établir immédiatement si une violation des données à caractère personnel s'est produite, afin d'en informer rapidement l'autorité de contrôle et la personne concernée ; **les actions de sensibilisation doivent être poursuivies systématiquement ; elles constituent un levier opportun pour promouvoir plus largement la cybersécurité** (**Recommandation 8**) grâce aux analyses d'impact mentionnées dans le RGPD.

Les particularités des domaines de la santé et de la finance ajoutent à ces difficultés générales des difficultés spécifiques.

- Si le RGPD définit de manière large la donnée personnelle de santé, il ne caractérise pas suffisamment celles qui sont indissociables de l'identité des patients et nécessaires à la pratique médicale. Le développement des appareils connectés de santé est le meilleur exemple du dilemme existant entre valeur ajoutée pour les citoyens et respect de la vie privée. Une bonne application du RGPD dans le secteur de la santé passe par **la définition des données médicales nécessitant une protection spécifique et plus forte que les autres données sensibles de santé** ; par ailleurs, comme le permet le RGPD[7], **le droit à l'effacement ne devrait pas s'appliquer à ces données** (**Recommandation 11**).

- Les activités de services financiers reposent beaucoup sur le traitement de données personnelles ; elles sont fortement régulées, souvent par des textes européens. Les établissements qui assurent des activités de tenue de comptes de paiement ont été soumis, dans le même calendrier, à la mise en œuvre de deux ensembles importants de règles : le RGPD et la deuxième directive sur les services de paiement (DSP2). Ces deux réglementations nouvelles ne semblent pas se contredire, bien qu'elles portent parfois sur des enjeux voisins. Mais, sans logique évidente, **les obligations de portabilité des données personnelles sont**

[7] cf. considérant 65 du RGPD : « Les personnes concernées devraient avoir le droit d'obtenir que leurs données à caractère personnel soient effacées et ne soient plus traitées […] Toutefois, la conservation ultérieure des données à caractère personnel devrait être licite lorsqu'elle est nécessaire […] pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques… »

considérablement plus exigeantes à l'égard des établissements teneurs de comptes de paiement qu'elles ne le sont à l'égard des autres entreprises, ce qui peut inviter à une **réflexion d'ensemble sur une différenciation des obligations de** portabilité selon la taille et la puissance de marché des entreprises (**Recommandation 3**). Par ailleurs, **une levée du secret entre l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) et la CNIL favoriserait la mise en œuvre du RGPD** (**Recommandation 14).**

Des opportunités apparaissent, évaluées à 1 milliard d'euros par an par la DGE, soit pour faciliter la conformité au RGPD, soit pour développer de nouveaux marchés :

- L**es organisations professionnelles ont un rôle clef à jouer** en promouvant à l'échelle sectorielle les bonnes pratiques et les modèles adaptés, en aidant les entreprises à mieux percevoir la valeur de leurs données et en identifiant, pour les faire arbitrer par le Comité européen de la protection des données, les divergences de pratique entre les Etats membres qui pourraient induire des biais concurrentiels (**Recommandations 1, 4, et 5**).

- Le RGPD peut favoriser l'émergence de solutions, voire de champions français, dans les technologies nouvelles, en matière de **cybersécurité, de chiffrement, de suppression des données, d'anonymisation des données, de traitement en local et d'obfuscation[8] et d'évaluation du risque de ré-identification** (**Recommandation 15**).

- **La certification et la labellisation** de systèmes d'information ou d'entreprises en matière de protection de données personnelles répondent à un besoin du secteur économique, et se développeront si un cadre général est défini par la puissance publique et harmonisé au niveau européen (**Recommandations 10 et 16**).

- Dans un contexte de pratiques inacceptables de certains grands acteurs internationaux et de piratages de données de grande ampleur, le RGPD, standard le plus exigeant dans le monde en matière de protection des données à caractère personnel, pourrait bien faire école à l'étranger. Être « *privacy friendly* » peut être un atout commercial et marketing par rapport à des concurrents non-européens. **Les entreprises européennes, premières confrontées à une telle norme, peuvent profiter de ce « *first-mover advantage* »** (**Recommandations 2 et 13**).

*
* *

[8] Stratégie de protection de la vie privée sur internet qui consiste à publier des informations fausses ou imprécises de manière à dissimuler les informations pertinentes (source Wiktionnaire)

TABLE DES RECOMMANDATIONS

Recommandations principales (niveau 1)

Recommandations spécifiques (niveau 2)

Recommandations spécifiques (niveau 3)

1 LES ENJEUX DU RGPD

1.1 Les objectifs, les grands principes et la démarche générale de la Commission

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est reconnue comme un droit fondamental, tant par la Charte des droits fondamentaux de l'Union européenne que par le traité sur le fonctionnement de l'Union européenne. La Commission européenne a proposé le 25 janvier 2012 une réforme des dispositions concernant la protection des données personnelles dans l'ensemble des pays de l'Union européenne : il s'agissait d'élaborer un nouveau compromis entre les droits des personnes et les intérêts légitimes des organisations publiques ou privées recourant au traitement de données à caractère personnel.

Cette réforme reposait sur deux volets :

- d'une part l'actualisation sous la forme d'un règlement des principes énoncés dans la directive européenne de 1995 sur la protection des données (mises à jour nécessaires concernant notamment les réseaux sociaux, le *cloud computing* ou encore le *Big Data*) ; il fallait en effet, selon la Commission européenne, surmonter l'insécurité juridique et les obstacles à une libre circulation des données qu'induisaient des différences de transposition entre les Etats membres ;
- d'autre part la rédaction d'une Directive[9] relative à la protection des données à caractère personnel entrant dans un cadre régalien (prévention et détection des infractions pénales, enquêtes et poursuites en la matière, exécution de sanctions pénales).

Le règlement général sur la protection des données du 27 avril 2016 (RGPD)[10] est entré en application le 25 mai 2018, en abrogeant la directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Les premiers considérants du RGPD lui donnent pour ambition de « *contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques* », et posent pour principe que « *le traitement des données à caractère personnel devrait être conçu pour servir l'humanité* ».

Toute donnée concernant un citoyen européen, même si elle est traitée en dehors de l'Union, est dans le champ d'application du RGPD. On ne peut transférer des données hors de l'Union sans certaines garanties. Depuis l'entrée en application du RGPD, on est passé d'une logique de déclaration et d'autorisation *a priori* à une logique de responsabilisation et de contrôle *a posteriori* des acteurs qui traitent des données à caractère personnel, assortie de sanctions. On notera qu'en France, 43 % des internautes considèrent que les données personnelles sont insuffisamment

---

[9] Directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

[10] Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)

protégées ; mais que 82 % d'entre eux ne sont pas prêts à payer pour que leurs données ne soient pas utilisées[11].

A côté du RGPD, qui régit le traitement de données personnelles, le règlement 2018/1807 du 14 novembre 2018[12] s'applique aux données qui ne présentent pas le caractère de données personnelles. Il prohibe, hors motif de sécurité public, toute exigence nationale de localisation des données. A compter du 28 mai 2019, date d'application du règlement 2018/1807, ce cadre dual, harmonisé et applicable de plein droit, assurera dans toute l'Union européenne la libre circulation des données, qu'il s'agisse ou non de données personnelles.

1.2 Les principales dispositions du RGPD

1.2.1 L'applicabilité du cadre juridique

L'article 2 du RGPD précise qu'il s'applique « *au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* ». La protection des données s'effectue idéalement dès la conception du produit ou service à deux niveaux (*privacy by design* et *privacy by default*). Certaines données, dites sensibles, ne peuvent être traitées qu'avec des garanties supplémentaires en raison des risques que leur traitement implique pour la vie privée ou pour les droits des personnes.

En vertu de son article 3, le RGPD « *s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union* ». Il s'applique également « *au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:*

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

1.2.2 Les principes du traitement des données à caractère personnel

Le RGPD pose le principe de la responsabilité du responsable du traitement[13] : « *le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* ».

L'article 5 du RGPD énonce les principes relatifs au traitement des données à caractère personnel :

- la loyauté du traitement (licéité, loyauté, transparence) ;
- la détermination d'une finalité et le respect de celle-ci (limitation des finalités) ;

---

[11] Baromètre du numérique CGE, ARCEP, Agence du numérique, 2018

[12] Règlement 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne

[13] Article 24 du RGPD

- l'obligation du caractère « *pertinent, adéquat et limité* » des données qui doivent être exactes et à jour (minimisation des données) ;
- la limitation de la durée de conservation des données ;
- la sécurité (intégrité et confidentialité) ;
- la responsabilisation (« *accountability* »).

1.2.3 Les droits issus du RGPD

Le RGPD consacre des droits fondamentaux en matière de protection des données à caractère personnel (voir Annexe 4 : Les droits fondamentaux issus du RGPD, p. 69) :

- le droit à l'information ;
- le droit d'accès aux données ;
- le droit de rectification ;
- le droit d'effacement ;
- le droit d'opposition ;
- le droit à la limitation du traitement ;
- le droit à la portabilité des données à caractère personnel fournies.

1.3 La loi « protection des données personnelles » du 20 juin 2018 et l'ordonnance du 12 décembre 2018

Le RGPD est d'application directe sur l'ensemble du territoire de l'Union Européenne (contrairement aux directives antérieures auxquelles il se substitue). Il prime donc sur la loi française et s'applique de plein droit depuis sa date d'application, le 25 mai 2018. Toutefois, le législateur français a dû intervenir pour abroger les dispositions nationales issues de la loi « informatique et liberté » du 6 janvier 1978 devenues contraires au RGPD.

De plus, le RGPD renvoie aux législations nationales de chaque Etat membre, par exemple en ce qui concerne le régime des sanctions pénales applicables en cas de violation des principes du règlement ; les violations, le montant maximal et les critères de fixation des amendes administratives ; ou encore les limitations au traitement des données génétiques, biométriques ou concernant la santé.

De telles « marges de manœuvres » octroyées aux Etats membres permettent aussi aux Etats de déroger ou de préciser certaines dispositions du RGPD, telles que l'âge à partir duquel des enfants peuvent être sujet à un traitement de données à caractère personnel sans le consentement d'un adulte responsable[14]. La liste de ces marges de manœuvre figure ci-dessous en Annexe 5 : Les « marges de manœuvre » autorisées par le RGPD, p. 71.

La loi du 20 juin 2018 relative à la protection des données personnelles[15] a donc adapté le cadre législatif national au RGPD :

- elle abroge de larges pans de la loi du 6 janvier 1978 (la Loi « Informatique et Libertés »[16]), dont la logique était différente de celle du RGPD ;

[14] Article 8 du RGPD

[15] Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles

[16] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (la « loi informatique et libertés »)

- elle transpose la directive 2016/680 du 27 avril 2016 (relative, comme on l'a vu, au traitement de données personnelles entrant dans le cadre d'activités régaliennes) ;
- elle exploite certaines des marges de manœuvre nationales offertes par le RGPD (cf. liste des choix français en Annexe 5 : Les « marges de manœuvre » autorisées par le RGPD).

Il est navrant que les adaptations de la loi française rendues nécessaires par le RGPD aient été finalisées postérieurement à l'entrée en application de ce règlement, plus de deux ans après sa publication le 4 mai 2016. Ce retard a sans doute été préjudiciable à la préparation des entreprises françaises et a constitué un mauvais signal.

Qui plus est, les changements apportés par la loi du 20 juin 2018 à la loi du 6 janvier 1978 produisaient un résultat si peu lisible que son article 32 habilitait le Gouvernement à prendre par ordonnance les mesures nécessaires, d'une part, à la réécriture de l'ensemble de la loi du 6 janvier 1978 « *afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence ainsi qu'à la simplicité de la mise en œuvre par les personnes concernées* » de ses dispositions ; d'autre part, « *pour mettre en cohérence avec ces changements l'ensemble de la législation applicable à la protection des données à caractère personnel, apporter les modifications qui seraient rendues nécessaires pour assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes, harmoniser l'état du droit, remédier aux éventuelles erreurs et omissions et abroger les dispositions devenues sans objet* ».

Tel est l'objet de l'ordonnance du 12 décembre 2018[17] prise en application de l'article 32 de la loi du 20 juin 2018. Ses dispositions entreront en vigueur au plus tard le 1er juin 2019. D'importantes dispositions réglementaires doivent encore être prises sous la forme d'un décret, qui modifiera le décret du 20 octobre 2005[18] et mettra enfin la CNIL en ordre de marche par rapport à son nouveau rôle, trois ans après la publication du RGPD et un an après son entrée en application.

L'article 1er de l'ordonnance du 12 décembre 2018 abroge l'intégralité des 72 articles de la loi du 6 janvier 1978 et leur substitue 128 articles nouveaux. Ce choix étonnant conduit à encore faire référence aux dispositions françaises d'adaptation du RGPD sous l'intitulé de la « loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », alors que ces dispositions n'ont plus grand-chose à voir avec les dispositions d'origine de la loi de 1978. Là encore, ce n'était peut-être pas le meilleur moyen de faire prendre conscience aux entreprises françaises du changement de paradigme intervenu à travers le RGPD en matière de protection des données personnelles : là où la loi informatique et libertés reposait sur une logique déclarative, le règlement adopte, lui, une logique de responsabilité (« *accountability* »).

---

[17] Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel

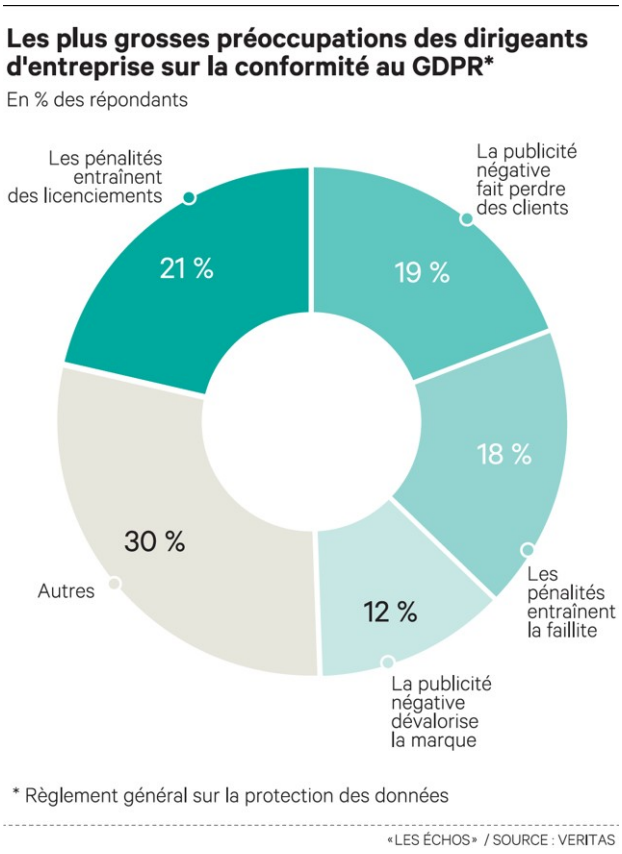
[18] Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

1.4 Le RGPD, source de risques et vecteur d'opportunités

1.4.1 Toutes les entreprises ne sont pas égales face à l'application du RGPD

Dans un environnement réglementaire peu lisible et dans un marché encore émergent d'offres de services liées à la mise en conformité des entreprises avec le RGPD, les offres d'audit et le conseil présentent une grande disparité des prix et de qualité. Ce manque de repères est source d'inquiétude au sein des entreprises, bien conscientes qu'une tension peut exister entre une interprétation maximaliste des exigences du RGPD et la bonne marche de l'entreprise.

Le RGPD n'affecte pas de la même manière les différentes entreprises. L'impact du RGPD ne dépend pas que de la taille de l'entreprise mais aussi du secteur d'activité, de l'importance des données collectées, du business model (il existe une grande inquiétude pour des petites startups dont le business est axé sur les données), ou encore de la relation au marché (B to B, B to C, B to B to C).



Par exemple, dans le secteur du e-commerce, les données personnelles occupent une place importante et le RGPD constitue un profond changement. Avant, la logique de déclaration paraissait simple à maîtriser. Désormais, l'analyse de conformité est au centre du processus et tout projet nécessite un minimum d'expertise (ce qui peut constituer une difficulté pour les PME). Les efforts à fournir compliquent la transformation digitale des entreprises.

1.4.2 Toutefois, le RGPD peut être créateur de croissance

La contrainte réglementaire du RGPD peut être transformée en opportunité si elle permet à une entreprise de se différencier de ses concurrents (affirmation d'une singularité et consolidation de la

confiance, différenciation concurrentielle). Le RGPD favorise la modernisation et la rationalisation des processus[19]. Il induit un nouvel équilibre entre la protection des utilisateurs et les intérêts des entreprises. Le RGPD devrait permettre une meilleure formalisation des échanges avec les sous-traitants (partage des responsabilités). Il favorisera la circulation des données à caractère personnel au sein de l'union européenne selon des règles communes et favorisera l'essor des activités liées au traitement des données personnelles.

1.5 L'harmonisation européenne

La CNIL, pendant un peu plus de 40 ans, au fil de ses délibérations et de l'exercice du rôle qu'elle a longtemps joué en amont de la mise en place de traitements de données personnelles, a édicté de nombreuses règles à caractère plus ou moins général.

A titre d'exemple, la décision d'autorisation unique n° AU-005[20] a défini une fois pour toutes et de manière exhaustive les données que les banques étaient autorisées à utiliser en France pour scorer les demandes de crédit : il leur était permis de distinguer les demandes selon le département de résidence du demandeur, mais pas selon sa commune de résidence. Exemple anecdotique mais révélateur : il a été interdit en France à une banque de tenir compte de la détention d'un animal de compagnie comme d'un indice de stabilité du foyer, alors que ce critère d'octroi de crédit était considéré comme légitime dans d'autres juridictions.

L'entrée en vigueur du RGPD a fait tomber toutes ces règles, puisqu'il est désormais de la responsabilité de chaque entreprise, aidée le cas échéant par son délégué à la protection des données, de recourir à telle ou telle donnée, de procéder à tel ou tel traitement. Pourtant, une certaine confusion semble subsister sur l'état du droit et sur la validité des règles anciennement édictées par la CNIL. D'aucuns craignent sans doute que la CNIL, dans son nouveau rôle de contrôleur *a posteriori*, se sente liée par les positions qu'elle a pu prendre dans un ordre juridique ancien et dans un rôle différent de contrôle *a priori*.

Il ne faudrait pas que ces ambiguïtés fassent obstacle à des innovations pertinentes. Il ne faudrait pas qu'elles induisent une distorsion de concurrence entre des acteurs anciens, plus soucieux de leur image, et des acteurs nouveaux, plus portés à l'expérimentation et à l'innovation. En dernier lieu, il ne faudrait pas, alors que le RGPD tend à l'harmonisation du marché unique, que des acteurs français soient entravés par des règles qu'ils seraient les seuls à observer, et dont leurs concurrents basés dans un autre Etat membre de l'Union s'affranchiraient.

La nouvelle logique de responsabilisation des acteurs, censée favoriser la prise d'initiative et l'innovation, engendre pourtant des craintes et des réticences, notamment en raison du montant élevé des sanctions potentielles en cas de non-respect du règlement. Nombreux sont ceux qui réclament des lignes directrices plus précises ou qui expriment le besoin d'être rassurés quant à la conformité de leurs traitements de données à caractère personnel.

---

[19] Intégration dans les projets cycle V ou agile et *privacy by design*, favorise une culture *User Experience*, de la qualité et de la sécurité

[20] Délibération n° 2006-019 du 2 février 2006 portant autorisation unique de certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit

Les mises en demeure et les sanctions prononcées par la CNIL sont encore peu nombreuses. Mais elles peuvent suffire à alimenter l'inquiétude et à faire craindre une remise en cause de certaines pratiques sectorielles. Cela a ainsi été le cas dans le secteur du ciblage publicitaire, après que la CNIL a publiquement mis en demeure une startup spécialisée dans la traque du parcours client à l'aide des données de géolocalisation des smartphones, au motif que le consentement des internautes n'avait pas été recueilli dans des conditions satisfaisantes (la procédure a été depuis clôturée)[21].

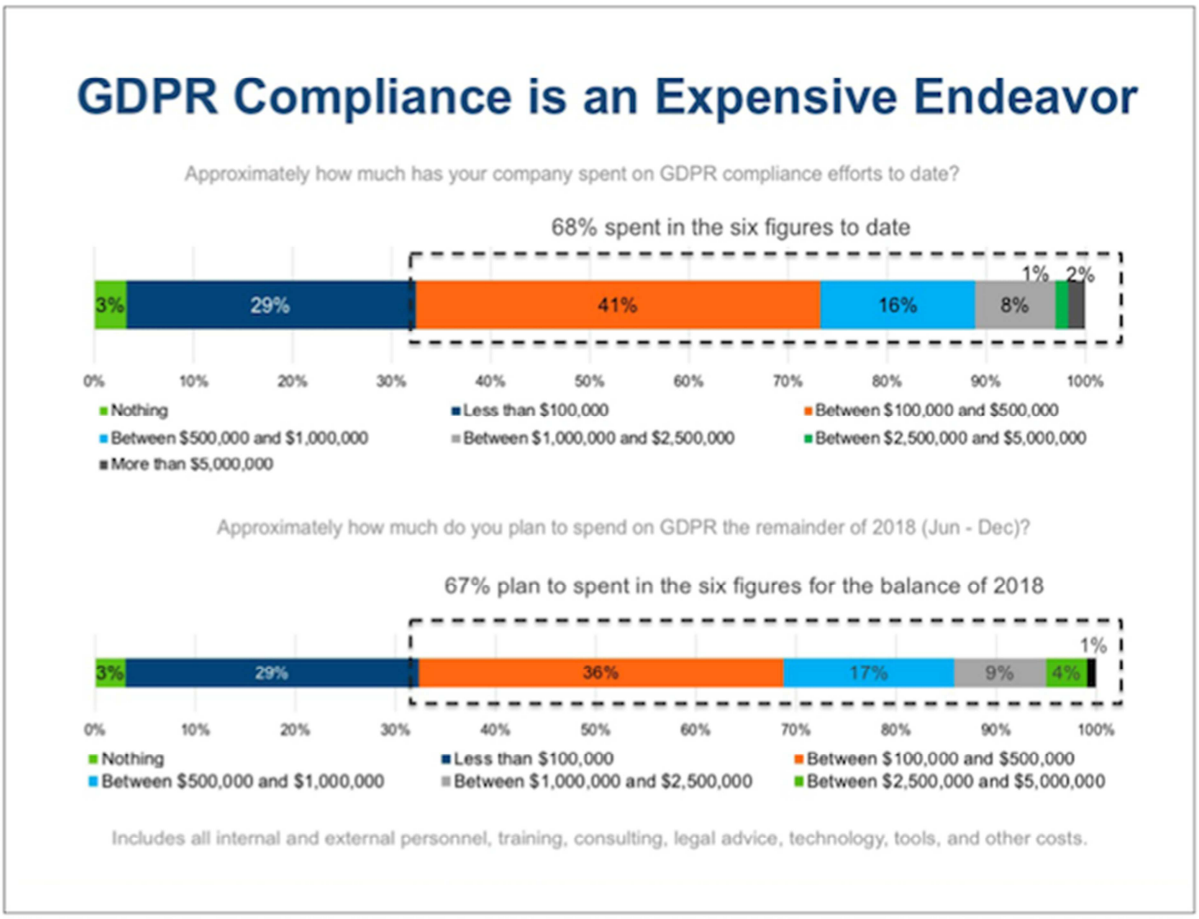
Dans toutes ces situations où les prescriptions du RGPD peuvent donner lieu à interprétation, où les cultures nationales varient et où elles ont pu donner lieu à des sur-transpositions des directives antérieures au RGPD, le comité européen de la protection des données et le mécanisme de contrôle de la cohérence de la mise en œuvre du RGPD au sein de l'Union européenne ont un rôle essentiel à jouer. Il est toutefois nécessaire que les fédérations professionnelles s'attachent préalablement à identifier les obstacles à un « level playing field » européen, afin qu'ils soient arbitrés en priorité par le comité européen de la protection des données.

Recommandation n° 1. [DGE] Inciter les fédérations professionnelles à identifier, en matière de traitement de données personnelles, les différences de règles entre les Etats membres qui pourraient induire des biais concurrentiels. [CNIL] Faire arbitrer ces différences par le Comité européen de la protection des données personnelles.

[21] cf. communiqués de la CNIL du 9 novembre 2018 et du 26 février 2019 :
https://www.cnil.fr/fr/applications-mobiles-mise-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire-2
https://www.cnil.fr/fr/applications-mobiles-cloture-de-la-mise-en-demeure-lencontre-de-la-societe-vectaury

2 DES DIFFICULTES GENERALES

Une étude TrustArc du 12 juillet 2018[22] révélait qu'un mois après l'entrée en vigueur du RGPD, 27 % seulement des entreprises européennes sondées (hors Royaume-Uni) se disaient prêtes et 49 % estimaient qu'elles le seraient à la fin de l'année 2018. Le coût de la conformité est significatif : comme l'illustre le diagramme ci-dessous[23], 68 % des entreprises ont dépensé plus de 100 000 dollars pour se mettre en conformité à la date d'entrée en vigueur du RGPD, le 25 mai 2018 (7 % des entreprises européennes ont même dépensé plus d'un million de dollars).



2.1 L'effacement des données et la portabilité constituent des droits nouveaux et coûteux à mettre en œuvre

2.1.1 Le droit d'accès ne soulève pas de difficulté nouvelle

Comme le prévoyait déjà la directive 95/46/CE du 24 octobre 1995, toute personne a le droit de savoir si elle est concernée par un traitement de données personnelles ; elle peut obtenir des

[22] https://www.trustarc.com/press/un-mois-apres-son-entree-en-vigueur-20-des-entreprises-declarent-etre-en-conformite-avec-le-rgpd/

[23] Source image : https://itsocial.fr/enjeux/securite-dsi/reglementation/cout-de-conformite-rgpd/

informations sur le traitement, ainsi qu'une copie des données la concernant et toute l'information disponible sur leur origine[24].

2.1.2 Le droit à l'effacement, une préoccupation des consommateurs

2.1.2.1 Un droit difficile à mettre en œuvre, mais prisé par une partie des consommateurs

Du point de vue des entreprises rencontrées par la mission, le droit à l'effacement[25] est difficile à mettre en œuvre mais prisé par une partie des consommateurs[26]. **Le droit à l'effacement est souvent invoqué comme principal poste des dépenses de mise en conformité avec le RGPD** : les bases de données n'ont en général pas été conçues avec cette préoccupation, les données relatives à un individu sont souvent dispersées dans une multitude de bases et de supports. Il faut donc faire des recherches, puis effectuer les suppressions de manière ciblée (penser aux exceptions au droit à l'effacement, respecter les délais de conservation) car les entreprises doivent conserver certaines données (obligations fiscales, comptables, sociales, etc.).

Le RGPD incite **à rationaliser et à optimiser** la collecte, le stockage et le traitement des données à caractère personnel. Même les startups créées depuis un petit nombre d'années sont en général confrontées à cette difficulté et le RGPD ne semble pas les avantager. A l'inverse, les nouvelles entreprises qui s'imposent d'emblée de respecter la notion de « *privacy by design* » prévue par le RGPD pourraient bénéficier d'un avantage compétitif.

Recommandation n° 2. [CNIL, ANSSI] Mettre en place des critères d'évaluation des méthodes d'anonymisation et d'effacement ciblé des données à caractère personnel.

2.1.2.2 …et une éventuelle opportunité

Dans la mesure où le RGPD impose que les données personnelles ne soient pas conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui excéderait celle nécessaire au regard des finalités pour lesquelles elles sont traitées, les entreprises seraient bien inspirées de définir a priori pour chaque donnée sa durée de conservation, ce qui faciliterait la mise en œuvre ultérieure du droit à l'oubli en anticipant la demande de suppression). Le processus de suppression des données pose essentiellement des problèmes d'ordre technique : retrouver les données, les supprimer n'est pas toujours facile pour les entreprises. Une voie possible est l'automatisation de la suppression des données : elle peut être une opportunité de développement d'activités de prestations de services aux entreprises.

[24] Article 15 du RGPD

[25] Article 17 du RGPD

[26] Existait déjà avec la directive 95/46/CE : conserver les données pour une durée adéquate

2.1.3 Le droit à la portabilité : des difficultés de mise en œuvre et des interrogations

2.1.3.1 Le droit à la portabilité est lourd à mettre en place

Le droit à la portabilité[27] permet à un consommateur de récupérer les données personnelles qu'il a confiées à un prestataire de services, que ce soit dans un but de vérification ou dans celui de les transférer chez un prestataire de service concurrent. Ce droit vise à favoriser un meilleur contrôle des données à caractère personnel par leurs propriétaires et à lever, lorsqu'elles existent, les barrières concurrentielles à l'entrée.

La mise en œuvre de ce droit a été l'un des chantiers de mise en conformité les plus laborieux du RGPD : le processus d'extraction des données peut être long et manuel car les données sont fréquemment dispersées à travers de nombreuses bases de données indépendantes, il n'existe pas de format standard de restitution des données et l'automatisation de la portabilité peut coûter cher à mettre en place. Au regard de ces efforts, le nombre des consommateurs qui font usage de ce nouveau droit est modeste.

La portabilité a été conçue pour faciliter aux consommateurs le changement de prestataires de services, notamment dans le cas de grandes entreprises telles que les GAFA ou les banques, dont les clients sont dans une certaine mesure captifs. Mais les entreprises plus petites ou dont le pouvoir de marché est moindre peuvent apparaître comme des victimes collatérales.

L'obligation de portabilité peut sembler trop uniforme : elle induirait dans le cas des petites entreprises une complexité inutile ; tandis que dans le cas de grandes entreprises en situation de quasi-monopole, le droit à la portabilité, insuffisamment exigeant, pourrait manquer son objectif. On notera à cet égard que les textes européens ont introduit des dispositions sectorielles beaucoup plus contraignantes que le droit à la portabilité dans le cas des services de paiement (cf. ci-dessous, chapitre 4.2 Les interactions entre le RGPD et la DSP2, p. 53).

La justification de la « portabilité renforcée » prévue en matière de services de paiement par la DSP2 est la suivante : les banques ont constitué au fil des années des bases de données extrêmement riches qui leurs procurent un avantage concurrentiel certain. La « portabilité renforcée » DSP2 a donc pour objet de permettre à de nouveaux entrants, les "fintechs", avec l'accord des clients concernés et par le biais d'API[28], de profiter de ces bases de données pour élaborer et offrir de nouveaux services. Ces dispositions, propres au marché des services de paiement, ne sont pas seulement propices à la concurrence : elles sont aussi favorables à l'innovation. Dès lors, il pourrait apparaître judicieux de les répliquer sur d'autres marchés où la collecte de données personnelles et la constitution de bases de données personnelles de taille significative constituent une barrière à l'entrée et la clé de l'innovation.

Recommandation n° 3. [DGE/DGTrésor] Envisager, à l'occasion de l'évaluation et de l'examen du RGPD en mai 2020, de différencier le droit à la portabilité selon la taille et le pouvoir de marché des entreprises, en exonérant de cette obligation les plus petites entreprises (*de minimis*) et en la renforçant (par exemple, par l'obligation de mettre en place une API) pour les plus grandes entreprises.

[27] Article 20 du RGPD

[28] Application Programming Interface

La formulation de l'article 20 du RGPD peut par ailleurs prêter à des interprétations divergentes : dans la mesure où le droit à la portabilité porte sur les seules « *données à caractère personnel fournies à un responsable du traitement* », certaines entreprises pourraient vouloir exclure du champ de la portabilité des données personnelles qui n'auraient pas été directement et explicitement fournies par la personne concernées : tel pourrait notamment être le cas des libellés d'opérations qui figurent dans les extraits de compte bancaire.

2.1.3.2 …mais il peut représenter un enjeu d'ouverture des marchés

Alors que le RGPD impose une restitution « *dans un format structuré, couramment utilisé et lisible par machine* » il n'existait évidemment pas d'emblée, à l'heure de l'entrée en vigueur du règlement, un consensus sur un tel format. Une standardisation des données et des formats doit certainement être poursuivie entre les entreprises de chaque secteur d'activité. **Il conviendrait d'encourager les responsables de traitement à se concerter avec leurs pairs afin de mettre en place des formats interopérables par secteur d'activité**[29]. Au regard du large éventail de types de données qui peuvent être traitées par le responsable du traitement, le règlement n'impose pas de formats spécifiques pour répondre à une demande de portabilité, si ce n'est que ce dernier doit être interopérable. L'une des autorités allemandes a décidé de travailler sur un schéma **d'interopérabilité par secteur d'activité**.

> **Recommandation n° 4.** [DGCCRF] Demander aux fédérations professionnelles/sectorielles de mettre en place un socle commun d'interopérabilité pour la portabilité des données par secteur d'activité //[CNIL] Mettre en place, au niveau européen, un cadre pour les standards d'échanges de données personnelles, et faire émerger des solutions logicielles françaises.

La mise en place de standards interopérables entre les entreprises – incitée par le RGPD – a pu intervenir spontanément dans certains cas (Google et Microsoft ont par exemple mis en place des outils permettant la portabilité), mais il s'agit d'un nouveau droit encore émergent, peu utilisé par les consommateurs. L'idée de la portabilité est qu'une substitution de prestataire de services peut être mise en œuvre simplement. **Il y a un potentiel en termes de concurrence et d'innovation qui est très intéressant pour les consommateurs et pour les nouveaux entrants**, le client ne doit être plus prisonnier d'un produit ou d'un autre prestataire de service (cf. infra Open Banking).

2.2 Les écueils liés au recueil du consentement, notamment dans le cas des traitements liés à la recherche et développement (R&D)

Selon les termes de l'article 6 du RGPD, un traitement de données à caractère personnel n'est licite « *que si, et dans la mesure où, au moins une des conditions suivantes est remplie :*

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

[29] Considérant 68 du RGPD

c) *le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;*

d) *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;*

e) *le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;*

f) *le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.* »

Le consentement n'est donc pas systématiquement requis pour assurer la collecte et le traitement de données personnelles. Mais, faute de lignes directrices ou d'une interprétation claire des dispositions ci-dessus, le recueil du consentement peut apparaître comme la manière la plus incontestable pour une entreprise de mettre ses pratiques en conformité avec le règlement.

Pour être valide toutefois[30], le consentement doit consister en une manifestation de volonté matérialisée par une déclaration ou par un acte positif clair ; il doit être libre (un choix réel, sans contrainte), spécifique (il correspond à des traitements et à des finalités déterminés), éclairé (les informations essentielles doivent être communiquées à la personne) et univoque (le consentement ne doit pas laisser pas place à l'ambigüité).

2.2.1 Le recueil du consentement de la personne peut représenter un obstacle

Recueillir le consentement de la personne n'est jamais évident. Les informations relatives aux politiques de confidentialité présentes dans les conditions générales d'utilisation (CGU) ne sont pas lues, ou seulement partiellement, dans 89 % des cas[31]. Les internautes les considèrent trop longues (80 %), non modulables (54 %) et peu claires (42 %).

Plusieurs difficultés doivent être surmontées :

- une entreprise peut avoir besoin de recueillir le consentement de ses clients à plusieurs traitements de natures différentes et pour des finalités différentes, de faire évoluer la liste de ses traitements selon ses besoins, de tenir compte de l'ancienneté variable des consentements recueillis et du succès incertain de leur réitération, de l'éventuelle révocation par certains clients de leur consentement… ce que seules l'élaboration et la gestion d'une base de consentements permet d'assurer ;
- un client a le droit de retirer son consentement à tout moment et il doit être aussi simple pour lui de retirer que de donner son consentement[32] ; mais en pratique il n'est pas simple d'assurer que les modalités de révocation du consentement soient aussi simples que celles du recueil du consentement ;

---

[30] Articles 4.11 et 7, considérant 32 du RGPD

[31] Synthèse du Rapport « Données personnelles et confiance : quelles stratégies pour les citoyens consommateurs en 2017 ? », Chaire Valeurs et Politiques des Informations Personnelles, Patrick Waelbroeck, Armen Khatchatourov, Claire Levallois-Barth, 23 juin 2017

[32] Article 7.3 du RGPD

- certains traitement de données personnelles sont particulièrement sensibles du point de vue des libertés et des droits fondamentaux (parce que les données pourraient révéler une prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ; ou parce que le traitement porte sur des données génétiques, des données biométriques, des données qui concernent la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique) ; il ne peut être dérogé à une interdiction de principe de tels traitements qu'au prix d'exigences renforcées, telles qu'un consentement donné de façon « explicite »[33] ;
- la latitude laissée par le RGPD aux États membres pour déterminer l'âge à partir duquel des enfants peuvent faire l'objet d'un traitement de données à caractère personnel, sans le consentement d'un adulte responsable, impose aux prestataires de services un traitement différencié selon le lieu de résidence de ces enfants.

Recommandation n° 5. [CNIL] Promouvoir auprès des fédérations professionnelles les bonnes pratiques par secteur pour le recueil du consentement. Favoriser la création de codes de conduite et leur application générale dans l'Union européenne, par la voie de l'adoption par la Commission d'un acte d'exécution (cf. article 40 du RGPD).

2.2.2 L'intérêt légitime et l'exécution du contrat, des dérogations trop vagues au recueil du consentement

Dans le cas d'un traitement mis en place dans « l'intérêt légitime » du responsable de traitement ou dans le cadre de l'exécution d'un contrat, le consentement n'est pas nécessaire. Pour que le traitement des données soit considéré d' « intérêt légitime », les utilisateurs doivent s'attendre raisonnablement à ce que le traitement soit réalisé avec leurs données. On peut imaginer que des finalités telles que la prévention de la fraude, la sécurité des réseaux ou, dans le cas des opérateurs de téléphonie mobile, la géolocalisation des utilisateurs seraient reconnues comme légitimes.

Il peut être tentant pour une entreprise d'utiliser sans discernement ces notions d' « intérêt légitime » ou d'exécution du contrat à des fins d'évitement du recueil du consentement, d'allègement de ses procédures et de ses charges, de meilleure fluidité de ses échanges avec ses clients. A rebours, il est probable que certaines entreprises, soucieuses d'éviter des risques de non-conformité avec le RGPD, se sont inutilement efforcées de recueillir le consentement de leurs clients à des traitements de données qui, à l'évidence, relevaient de l'intérêt légitime ou de l'exécution du contrat.

Ainsi, l'absence de lignes directrices sur l'interprétation de ces notions est susceptible d'induire des distorsions de concurrence. Ce serait tout particulièrement le cas si les autorités nationales chargées de la police du RGPD (la CNIL et ses homologues des autres Etats-membres) ne partageaient pas une même approche, ce qui pourrait bien advenir compte-tenu de traditions nationales assez différenciées en matière de respect de la protection des données personnelles.

Il existe donc de forts enjeux de clarification, qui pourraient être traités soit dans le cadre des mécanismes de coopération et de cohérence institués par le RGPD, à travers le rôle du Comité européen de la protection des données[34], chargé d'examiner toute question portant sur l'application du RGPD et de publier des lignes directrices, des recommandations et des bonnes pratiques afin d'en

[33] cf. considérant 51 et article 9 du RGPD

[34] cf. article 68 du RGPD

favoriser l'application cohérente ; soit à travers l'élaboration de codes de conduite paneuropéens[35], qui seraient rendus applicables dans toute l'Union européenne si la Commission les approuvait et les publiait sous la forme d'un acte d'exécution.

Recommandation n° 6. [CNIL] Clarifier les critères d'appréciation de l'intérêt légitime d'un traitement, de son rattachement à l'exécution d'un contrat, ou de la nécessité de mise en œuvre du recueil du consentement. Garantir une mise en œuvre cohérente de ces critères à travers l'Union européenne par leur publication par le Comité européen de la protection des données sous une forme appropriée.

2.2.3 Les modalités de recueil de consentements peuvent faire obstacle à l'innovation

Comme on l'a vu, l'article 5 du RGPD pose que les données à caractère personnel doivent être : a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ; b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ; d) exactes et, si nécessaire, tenues à jour ; e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel.

Ces principes tendent à inciter les entreprises à ne conserver et à ne travailler que sur des données dont l'utilité est prouvée. Mais on ne peut innover que si l'on procède à des tests, au moins dans une première phase. En particulier, le RGPD viendrait directement contrarier le recours au *Big Data* si les données analysées par ce moyen devaient avoir fait l'objet d'un consentement éclairé à un stade où les finalités sont encore incertaines. Le potentiel du *Big Data* et de l'intelligence artificielle repose sur l'accumulation de données à des fins d'analyse des corrélations et d'exploitation d'éventuels facteurs prédictifs (sans que la finalité ex-ante soit toujours anticipée).

Il devrait être admis et reconnu, sans dénaturer l'esprit du RGPD, qu'une entreprise peut légitimement accumuler des données, sans pouvoir justifier d'emblée d'une autre finalité que celles de la recherche et développement (R&D) et du développement de nouveaux produits ou services.

Recommandation n° 7. [CNIL] Afin de promouvoir l'innovation, le Comité européen de la protection des données devrait publier des lignes directrices indiquant clairement à quelles conditions et dans quelle mesure la R&D peut constituer un intérêt légitime permettant aux entreprises innovantes de procéder à des traitements de données personnelles, avant que ces traitements, s'ils débouchent sur de nouvelles offres de produits ou de services, et donc une nouvelle finalité, donnent lieu au recueil du consentement des clients.

[35] cf. article 40

2.3 La gestion des durées de conservation

Le RGPD prévoit que les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités du traitement[36]. Or, il n'existe pas une durée unique de conservation des données selon leur type ou leur nature, mais bien autant de durées que de finalités. Certaines données n'ont pas besoin d'être conservées pendant une durée supérieure à leur utilisation effective (quelques minutes à quelques jours). En revanche, d'autres catégories de données personnelles doivent être conservées pendant une durée fixée par la loi.

2.3.1 L'articulation du RGPD avec d'autres obligations légales concernant les durées de conservation est un faux problème

Si le caractère contraignant de la limitation de la conservation des données est évident (le droit américain semble permettre une conservation des données sans limitation de durée), la question de l'articulation entre le RGPD et des obligations légales ne se pose pas. En effet, l'article 17 du RGPD précise que le droit à l'oubli ne s'applique pas dans la mesure où le traitement est nécessaire *« pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* ».

Le RGPD assure donc qu'il est légitime de collecter les données s'il y a une justification légale[37] (par exemple, dans le cadre de la lutte contre la fraude et le blanchiment[38]). Dans le doute, la décision irréversible d'effacer une donnée personnelle peut être difficile à prendre, du fait d'un risque de ne plus pouvoir répondre à une obligation (par exemple dans le cadre d'un contrôle fiscal ou URSSAF). Avec une acuité variable selon le secteur d'activité, l'impossibilité de répondre favorablement à l'effacement des données d'un client du fait d'obligations étrangères au RGPD peut être complexe à justifier vis-à-vis de certains clients.

2.3.2 La gestion du stock de données antérieures au 25 mai 2018 a pu être une source de difficultés

Le manque de lignes directrices sur les conditions de reprise et de gestion du stock de données antérieures au 25 mai 2018 a pu gêner certains acteurs.

2.4 L'obligation de déclarer les failles du système d'information (SI)

80 % des entreprises ont constaté au moins une cyberattaque au cours des douze derniers mois[39]. Le responsable de traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre la « *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*

---

[36] Article 5.1 et considérant 39 du RGPD

[37] Article L561-12 du Code Monétaire et Financier relatif à l'obligation de conservation et d'archivage des données d'identité, d'opérations et de diligences de conformité

[38] Article L521-6 du Code monétaire et financier

[39] http://www.keep-watch.com/news.php

autorisé à de telles données »[40]. La définition juridique de « violation de données » recouvre deux notions : l'intrusion dans un système de traitement, et les conséquences de cette intrusion.

L'obligation de sécurité dont le responsable de traitement est le garant est une obligation de moyens et non de résultat[41] : il doit être en mesure de montrer que les mesures mises en place sont suffisantes, raisonnables et adaptées.

2.4.1 La sécurité, une difficile nécessité

2.4.1.1 Si les objectifs sont clairs, des zones d'ombres subsistent quant aux moyens à mettre en œuvre

Avec le RGPD, l'obligation qui pèse sur le responsable de traitement est une obligation de moyens et non une obligation de résultat. Le choix des mesures à prendre n'est pas précisé, il doit tenir compte des risques pesant sur les données. En cas de violation de la sécurité des données, le juge ou la CNIL recherchera si le responsable de traitement avait pris les mesures de sécurité raisonnables au vu du risque. Même lorsque des règlements types en vue d'assurer la sécurité des systèmes ont été élaborés dans le passé[42], les textes donnent aujourd'hui au responsable du traitement le choix des solutions techniques à adopter, du moment qu'il satisfait à son obligation de moyens dans la sécurisation des données[43].

2.4.1.2 Un chantier laborieux

Le repérage des traitements qui ne sont pas assez sécurisés, la formation des acteurs concernés et la gestion optimisée du cycle de vie des données dans le système d'information sont des étapes coûteuses du processus de mise en conformité. Mais, ce faisant, le RGPD peut favoriser une prise de conscience tout-à-fait bienvenue des enjeux de cyber-sécurité, au-delà de la seule protection des données des données personnelles.

Le RGPD entraîne des changements de principes dans l'élaboration des systèmes d'information (*privacy by design*, *privacy by default*, etc.). Ces principes sont difficiles à mettre en œuvre pour des entreprises disposant d'un système ancien (comme par exemple les grandes banques). Les PME et ETI restent les moins sensibilisées aux risques de cyberattaques.

Comme l'illustre le schéma[44] ci-dessous, alors que la cybersécurité est une source d'inquiétude pour les PME françaises (pour 76 % d'entre elles) et que le RGPD devait favoriser la prise de conscience du risque de sécurité informatique, 45 % des PME françaises n'ont pas renforcé leurs mesures de sécurité suite à l'entrée en vigueur du règlement.

---

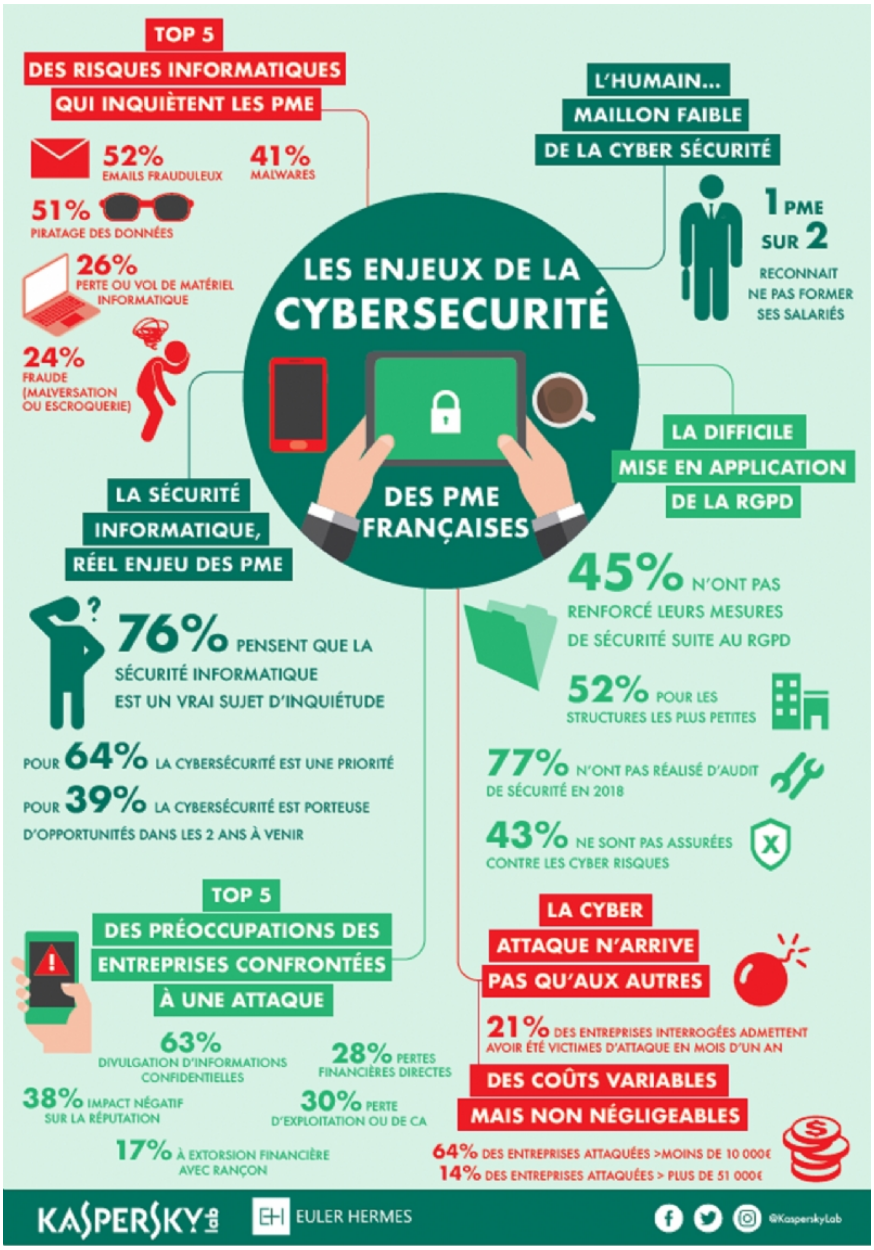
[40] Article 4.12 du RGPD

[41] Considérant 49 du RGPD

[42] cf. délibération n° 81-094 du 21 juillet 1981 de la CNIL portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques

[43] RGPD et droit des données personnelles, Fabrice Mattatia, 2018, Eyrolles

[44] Source image : https://www.kaspersky.fr/blog/pme-enjeux-cybersecurite/11244/



Recommandation n° 8. [ANSSI, ACYMA, CNIL] Créer des synergies entre les campagnes de sensibilisation auprès des PME sur le RGPD et sur la cybersécurité.

2.4.2 …mais un enjeu vital considéré comme tel

Un respect exigeant des règles de protection des données à caractère personnel permet aux entreprises de se différencier. Aujourd'hui, 25 % des Américains déclarent qu'ils ne travailleront plus avec une entreprise qui a fait l'objet d'une violation de données importante et 60 % travailleront moins avec une entreprise qui a laissé fuiter des données[45].

[45] Source : entretien Crédit Agricole

Le RGPD s'inscrit dans une perspective plus générale : le « capital donnée » dans une économie numérique a de la valeur et doit être protégé. La protection des données, la sécurité informatique et le respect de la vie privée sont capitaux. Ce règlement favorise une meilleure collecte de la donnée pour un meilleur conseil et pour un meilleur service pour le client.

De nombreux acteurs se positionnent sur le volet de la sécurité, en tant qu'offreurs de solutions concrètes de sécurité ou de formation (entreprises, université). Le respect de l'article 32 du RGPD, consacré à la sécurité du traitement, implique le déploiement d'outils, de guidelines et de formations. Le « hub sécurité » de la CNIL, qui comporte des conseils aux entreprises sur les bonnes pratiques en matière de sécurité ou de traitement des risques, peut y contribuer.

La CNIL et l'ANSSI cherchent à promouvoir une offre de conseil aux entreprises, notamment aux plus petites, sur l'acculturation à la cyber-sécurité. Toutes les entreprises sont susceptibles d'être victimes d'une cyberattaque, l'enjeu est général (espionnage industriel, etc.). Le RGPD, dès lors qu'il s'applique à toutes les entreprises et qu'il est assorti de sanctions, constitue un levier opportun pour élever le niveau général de cyber-sécurité.

La CNIL propose un processus de gestion des incidents de sécurité détaillé sur son site. Elle rappelle les bonnes pratiques permettant de prévenir les failles du système d'information et de garantir un niveau de sécurité adapté aux risques (pseudonymisation, chiffrement, réalisation d'audits de sécurité, de tests élémentaires, etc.).

La CNIL met également à la disposition des responsables de traitement un outil d'analyse d'impact PIA (*privacy impact assessment*), afin de créer des modèles d'analyse d'impact relative à la protection des données. L'ANSSI, quant à elle, dispose d'outils pour tester la vulnérabilité des systèmes d'information à une cyber-attaque.

2.5 Les relations avec les sous-traitants

Le RGPD régit pour la première fois les relations entre donneur d'ordre et sous-traitant, lorsqu'elles impliquent le traitement de données personnelles. Le sous-traitant doit désormais traiter les données à caractère personnel pour le compte du responsable de traitement, et sous ses ordres[46]. Le sous-traitant ne définit ni la finalité du traitement ni les moyens essentiels du traitement. En cas de manquement, le RGPD engage tant la responsabilité du donneur d'ordre que celle du sous-traitant (principe de coresponsabilité). Le RGPD impose que les relations entre responsable de traitement et sous-traitant de données soient strictement encadrées et formalisées dans un contrat écrit[47].

Toutefois, dans certains cas, un régime de co-responsabilité de traitement entre plusieurs entreprises peut être institué. Un sous-traitant technique peut donc être, au regard du RGPD, soit un sous-traitant de données personnelles, soit un co-responsable du traitement de données personnelles.

[46] Article 4.8 du RGPD

[47] Article 28 et considérant 81 du RGPD

2.5.1 Une difficulté à caractériser et le statut des sous-traitants

2.5.1.1 Une interdépendance nouvelle des acteurs

Dans le régime antérieur d'autorisation a priori, la responsabilité du donneur d'ordre primait, le sous-traitant était plus ou moins à l'abri des sanctions. Ce n'est plus le cas avec le RGPD qui institue une chaîne de responsabilité entre le responsable de traitement et les sous-traitants en renforçant les obligations contractuelles. La marge de manœuvre dont dispose un sous-traitant est limitée. La sous-traitance dans le RGPD concerne une multitude d'acteurs pour lesquels il est parfois difficile d'établir le degré de responsabilité (cf. à cet égard l'arrêt rendu par la CJUE dans une affaire où il s'agissait de départager les responsabilités entre Wirtschaftsakademie Schleswig-Holstein GmbH et Facebook Ireland Ltd[48]).

La sous-traitance « classique » consiste à faire exécuter à un sous-traitant diverses tâches dans le respect d'un cahier des charges. Mais parfois un prestataire, de par ses compétences techniques et son pouvoir de marché, dispose d'une forte autonomie et peut être qualifié de « *personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ». Dans cette hypothèse, il n'est pas un sous-traitant de données personnelles puisqu'il a un rôle actif autonome mais un responsable du traitement des données personnelles à part entière, au même titre que le donneur d'ordre (il y a donc deux responsables de traitements, qui sont « co-responsables »).

L'article 26 du RGPD dispose que « *les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée (…) par voie d'accord entre eux* » mais également que « *les grandes lignes de l'accord sont mises à la disposition de la personne concernée* ». Il est fréquent qu'en pratique les co-responsables de traitement se partagent une base de données commune pendant la durée de la relation contractuelle qui les unit. Cependant une fois cette relation contractuelle terminée, la question de la propriété de la base de données peut poser des difficultés.

Recommandation n° 9. [Délégués ministériels à la protection des données] Veiller à la conformité avec le RGPD de l'ensemble des contrats de sous-traitance souscrits par l'Etat.

2.5.1.2 Des obligations parfois problématiques

Avec le RGPD, on bascule dans une logique de responsabilisation de tous les acteurs impliqués dans le traitement des données personnelles. Si certaines obligations ne posent pas de problèmes particuliers dans le cas de la sous-traitance et relèvent d'une simple application du règlement (obligation de transparence, protection des données, avertissement au responsable de traitement d'une violation de données[49], désignation d'un DPO[50], élaboration d'un registre de traitement[51],

[48] CJUE affaire C-210/16 « Wirtschaftsakademie » du 5 juin 2018

[49] Article 33 du RGPD

[50] Article 37 du RGPD

licéité des transferts de données, aide et conseil au responsable de traitement, choix et conseil du sous-traitant[52], etc.), d'autres soulèvent des questions.

En tête des préoccupations de mise en conformité des entreprises avec le RGPD figurait la renégociation des contrats existants. La responsabilisation du sous-traitant implique que le contrat détaille les responsabilités de chacun ; des renégociations systématiques ont donc été nécessaires avec les sous-traitants. Les contrats en cours d'exécution ont dû être modifiés et renégociés pour inclure les clauses obligatoires prévues par le RGPD. Ces renégociations ont pu être lourdes à mettre en place, et leurs conséquences ont été largement sous-estimées par les entreprises :

- les nouvelles conditions de responsabilité avec le sous-traitant impliquent une discussion commerciale : certains, davantage responsabilisés (et souvent réticent à se voir attribuer des responsabilités), réclament de meilleures conditions et/ou rémunérations ;
- parfois le nombre de contrats de sous-traitance externe a été très élevé (jusqu'à 2500 pour une grande banque française par exemple) ;
- se pose la question du rôle joué par le sous-traitant (par exemple : que font Windows ou Facebook avec les données personnelles ?) Il a fallu aussi regarder toutes les prestations, les identifier ou non en tant que sous-traitance et renégocier les contrats. C'est d'autant plus complexe qu'il ne s'agit pas forcément de données personnelles (pas la même utilisation pour tous les usagers) ;
- chaque donneur d'ordres d'un même sous-traitant peut défendre sa propre compréhension du RGPD et formuler des demandes différentes. Il est d'autant plus difficile de les satisfaire qu'il y a une asymétrie de taille entre les partenaires. Le RGPD a pu induire des changements de partenaires, pour des seules raisons de conformité au RGPD, au risque de conséquences sur la bonne marche des opérations.

Ce point a été sous-estimé pour plusieurs raisons :

- il n'est pas toujours évident de qualifier le rôle de chaque acteur ;
- deux annexes aux contrats de sous-traitance sont importantes et nécessitent une documentation précise : l'une décrit le contenu des traitements et l'autre les dispositions de sécurité ;
- la responsabilité du sous-traitant est accrue, avec des sanctions beaucoup plus importantes. La renégociation des contrats en cours a pu être longue, en particulier avec des acteurs à l'étranger pas toujours sensibilisés aux exigences du RGPD.

Une autre préoccupation est liée au respect des obligations de sécurité des données confiées à un sous-traitant. Bien que les conditions de sécurité du traitement doivent être explicitées et verrouillées par le contrat[53], quand les sous-traitants sont de tailles et de statures très différents, le niveau effectif de sécurité est fortement tributaire des ressources humaines et techniques du sous-

---

[51] Article 30 du RGPD

[52] Article 28 du RGPD

[53] Article 24 du RGPD

traitant. Une attention toute particulière doit être allouée au transfert de données, difficilement sécurisable et très fréquent (utilisation d'un Cloud, hébergement des données, etc.).

Enfin, une dernière préoccupation est liée au recours par un sous-traitant à un sous-traitant de second rang. Si la démarche est bien encadrée par le RGPD[54], elle implique d'une part que le sous-traitant initial se rende responsable vis-à-vis du responsable de traitement si le nouveau sous-traitant ne respecte pas ses obligations, et d'autre part que le responsable de traitement identifie précisément la chaîne de sous-traitance (hébergement des données, transfert des données, localisation des données, etc.) en connaissant l'intégralité des acteurs qui entrent en ligne de compte dans le traitement des données.

2.5.2 Les moyens d'encadrer au mieux les relations de sous-traitance

2.5.2.1 Les clauses contractuelles types

Les contrats entre donneur d'ordre et sous-traitant peuvent théoriquement[55] s'appuyer sur des clauses contractuelles types établies par la Commission : « *Le responsable du traitement et le sous-traitant peuvent choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence, puis par la Commission* »[56].

Mais ces clauses contractuelles types n'existaient pas à l'heure où elles auraient été le plus utiles, lorsqu'il s'est agi pour les entreprises de mettre l'ensemble de leurs contrats en conformité avec le RGPD, au cours des mois qui ont précédé l'entrée en application du règlement.

2.5.2.2 Les règles d'entreprise contraignantes (ou « binding corporate rules »), un outil au service de la conformité

Un groupe multinational (ou un groupe d'entreprises multinationales engagées dans une activité économique conjointe) peut se doter d'un corps de règles qui définissent sa politique en matière de transferts internes de données, même lorsque ces transferts sont en direction ou en provenance de pays non soumis au RGPD.

Ces règles d'entreprise contraignantes (« binding corporate rules » ou BCR)[57] peuvent être approuvées par la CNIL, ou par toute autre entité homologue d'un autre Etat membre de l'Union européenne agissant comme autorité chef de file, pour autant que ces règles incluent tous les principes essentiels et les droits opposables prévus par le RGPD.

Ce qui s'apparente alors à un « règlement général sur la protection des données interne à un groupe d'entreprises » facilite la mise en œuvre du RGPD là où il s'impose et étend, de manière globale et uniforme, l'application du règlement aux implantations du groupe multinational dans des pays tiers (tels que les Etats-Unis ou d'autres pays n'assurant pas un niveau de protection équivalent à celui de l'Union européenne).

---

[54] Article 28.4 du RGPD

[55] Article 28.7 du RGPD

[56] Considérants 81 et 109 du RGPD

[57] Article 47 du RGPD

Les règles d'entreprise contraignantes sont définies comme « *les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe* »[58].

Les BCR permettent, selon la CNIL :

- d'être en conformité avec les principes du RGPD ;
- d'éviter de conclure autant de contrats qu'il existe de transferts au sein d'un groupe ;
- d'uniformiser les pratiques relatives à la protection des données personnelles au sein d'un groupe ;
- de communiquer sur la politique d'entreprise en matière de protection des données personnelles auprès de ses clients, partenaires et salariés et de leur assurer un niveau de protection satisfaisant lors des transferts de leurs données personnelles ;
- de placer la protection des données au rang des préoccupations éthiques du groupe**.**

2.6 Le traitement des données liées aux relations de travail

2.6.1 Un cas d'école pour l'application du nouveau règlement

Concernés directement ou indirectement par une grande variété de données personnelles relatives aux salariés, les services de ressources humaines sont particulièrement concernés par la mise en œuvre du RGPD, quelles que soient la taille et le secteur d'activité de l'entreprise.

Tout employeur est en effet amené à manipuler un champ plus ou moins large de données à caractère personnel attachées à son personnel : adresse, coordonnées bancaires, numéro de sécurité sociale, absentéisme (arrêts maladie, événements familiaux…), accidents du travail, déclarations sociales obligatoires, registre du personnel, sanctions disciplinaires, contrôle d'accès, annuaire comportant des photographies des salariés, dispositifs individualisés de suivi de la performance, géolocalisation, télésurveillance, écoute et enregistrement des conversations téléphoniques...

Le règlement ouvre dans le domaine des ressources humaines des marges de manœuvre nationales dont l'Etat français ne semble pas avoir fait usage :

« *Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et*

[58] cf. la notice exposée sur le site de la Commission européenne https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_fr

de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.

Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail. »[59]

2.6.2 Des impacts limités sur les pratiques des services de ressources humaines

En réalité, le règlement ne fait pas véritablement novation par rapport aux pratiques existantes. Les obligations de l'employeur ne sont pas différentes des autres responsables de traitement. C'est ainsi le cas des obligations d'informations relatives aux droits et à leurs modalités d'exercice, qui sont toutefois facilitées dans le cas des relations du travail par l'existence de supports variés : règlement intérieur, contrat de travail, notes de service, etc.

Les instances du personnel peuvent utilement être associées à la mise en conformité au RGPD (implication dans une charte informatique, un règlement intérieur par exemple), mais il s'agit d'une meilleure pratique plutôt que d'une obligation.

Les partenaires sociaux devraient intégrer dans les conventions collectives de branche ou dans des accords interprofessionnels des règles relatives au traitement des données à caractère personnel des salariés.

Les données RH renvoient plus particulièrement à trois problématiques spécifiques :

- la durée de vie des données personnelles : conservation des documents, durée du contrat de travail ;
- la mise à jour ou l'effacement des données, du recrutement à la rupture du contrat de travail ;
- la pertinence des données demandées et traitées : documents demandés pour l'embauche, gestion des relations avec des partenaires extérieurs, BDES[60], obligations contractuelles et légales (notamment au niveau fiscal et social).

Le rapport d'activité 2017 de la CNIL[61] rapporte que 16 % des plaintes déposées concernent les ressources humaines. Ces demandes proviennent de salariés, de syndicats ou d'inspecteurs du travail. Elles concernent principalement, par ordre décroissant, les dispositifs de vidéosurveillance, les dispositifs de géolocalisation, l'accès au dossier professionnel, l'accès à la messagerie professionnelle des salariés absents ou ayant quitté l'entreprise et la sécurité des données.

Des anomalies peuvent aussi tenir à la collecte de données non pertinentes, notamment lors du recrutement (collecte de données superflues lors du processus de recrutement, conservation des données relatives à des candidats non embauchés, etc.).

---

[59] Article 88 : Traitement de données dans le cadre des relations de travail ; cf. aussi le considérant 155 La protection des données RH n'est pas nouvelle, elle était déjà évoquée dans la loi du 6 janvier 1978

[60] Base de données économiques et sociales : http://www.tissot-formation.fr/rgpd-des-consequences-sur-la-bdes-6603984/

[61] https://www.cnil.fr/sites/default/files/atoms/files/cnil-38e_rapport_annuel_2017.pdf

Si le RGPD défend un parti-pris de minimisation des données personnelles, la collecte, le traitement et la durée de conservation des données repose dans de nombreux cas sur des obligations légales à la charge des entreprises[62] :

Type de document	Durée de conservation	Texte de référence
Bulletin de paie (double papier ou sous forme électronique)	5 ans	Article L. 3243-4 du code du travail
Registre unique du personnel	5 ans à partir du départ du salarié	Article R. 1221-26 du code du travail
Document concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régimes de retraite.	5 ans	Article 2224 du code civil
Document relatif aux charges sociales et à la taxe sur les salaires	3 ans	Articles L. 244-3 du code de la sécurité sociale et L. 169 A du livre des procédures fiscales
Comptabilisation des jours de travail des salariés sous convention de forfait	3 ans	Article D. 3171-16 du code du travail
Comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation	1 an	Article D. 3171-16 du code du travail
Observation ou mise en demeure de l'inspection du travail Vérification et contrôle du CHSCT	5 ans	Article D. 4711-3 du code du travail
Déclaration d'accident du travail auprès de la caisse primaire d'assurance maladie	5 ans	Article D. 4711-3 du code du travail

2.7 Les PME/TPE : une difficulté économique et un manque d'information

2.7.1 Au même titre que les autres entreprises, les PME/TPE sont concernées par le RGPD

Toutes les entreprises qui collectent des données personnelles de personnes résidant sur le territoire européen sont concernées par le RGPD. Le règlement s'applique de la même manière dans le secteur public et dans le secteur privé et vaut aussi bien pour les grandes entreprises que pour les PME et TPE, quelles que soient la taille ou le nombre de salariés.

La mise en conformité touchant de manière transversale tous les services (aussi variés que les ressources humaines ou le système d'information), indépendamment de la taille des entités, le RGPD peut représenter pour les PME/TPE un chantier relativement coûteux. Pour les aider dans cette démarche, Bpifrance en partenariat avec la CNIL a élaboré un guide[63]. Ce dernier explique ce qu'est le RGPD et son utilité. L'action, modeste mais louable, devrait être prolongée pour accompagner les PME/TPE.

[62] https://www.service-public.fr/professionnels-entreprises/vosdroits/F10029

[63] https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

2.7.2 Il existe cependant des spécificités propres aux PME/TPE, notamment en ce qui concerne le registre de traitement

Si le règlement s'applique donc aux PME et TPE, un souci de proportionnalité est pris en compte dans le RGPD : « *les institutions et organes de l'Union, et les États membres et leurs autorités de contrôle sont […] encouragés à prendre en considération les besoins spécifiques des micro, petites et moyennes entreprises dans le cadre de l'application du présent règlement* »[64].

La CNIL indique que « *les entreprises de moins de 250 salariés bénéficient d'une dérogation en ce qui concerne la tenue de registres* » (cf. Annexe 8 : Le registre de traitement des données à caractère personnel, p. 87). Ils doivent inscrire au registre les seuls traitements de données suivants :

- les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ;
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.) ;
- les traitements qui portent sur des données sensibles (exemple : données de santé, infractions, etc.).

En pratique, la tenue de registres est donc réservée aux traitements à caractère exceptionnel (par exemple, une campagne de communication à l'occasion de l'ouverture d'un nouvel établissement, sous réserve que ces traitements ne soulèvent aucun risque pour les personnes concernées). En cas de doute sur l'application de cette dérogation à un traitement, la CNIL recommande de l'intégrer dans le registre.

2.7.3 Faire de ces spécificités des opportunités ?

Le RGPD représente pour les PME un facteur de transparence et de confiance. Comme il est moins fréquent pour les PME/TPE d'être mieux-disant en matière de conformité au RGPD, faire partie des « *first movers* » peut être un élément de différenciation intéressant. Cette différence peut notamment jouer pour les PME/TPE ayant des accords commerciaux avec des grands groupes : il y a fort à parier que ces derniers donneront la priorité aux PME/TPE en pointe vis-à-vis du RGPD.

Le texte oblige en effet toute entreprise à s'assurer que tous les acteurs entrant en jeu dans le processus de traitement de données à caractère personnel respectent le RGPD. Ainsi, une bonne conformité avec le RGPD pour les PME/TPE est une opportunité de se démarquer de la concurrence. Cette dimension de fidélisation par la confiance concerne également les clients directs et pas uniquement le *B to B* (bonne image, réputation).

Les PME/TPE peuvent profiter de la possibilité de mutualisation offerte par le RGPD concernant le DPO afin de limiter les coûts et les risques. Elles peuvent également partager des fonctions DAF. Pour les PME/TPE, il est donc possible d'externaliser et de mutualiser pour gagner en efficacité et en rentabilité.

---

[64] Considérant 13 du RGPD

3 LE SECTEUR DE LA SANTE

La notion de « donnée personnelle » portée par le RGPD, l'absence de celle de « donnée de santé », ouvre dans la santé une problématique particulière qu'il est nécessaire d'instruire pour bien comprendre les enjeux et les difficultés spécifiques d'application du RGPD dans ce secteur.

La place des données de santé dans **l'activité soignante** est indissociable de l'identification du patient. Ceci mérite d'autant plus l'attention que le numérique pénètre la santé. Les nouveaux **outils numériques** ainsi mobilisés introduisent de nouvelles formes de valorisation de ces données.

Telles sont les spécificités du secteur qui méritent attention et sont développés dans cette partie.

3.1 Donnée personnelle ,,,,,, donnée de santé

Souvent utilisées dans le droit français, les expressions « données de santé » et « données de santé à caractère personnel » ne font pourtant l'objet d'aucune définition précise. Ni la loi de 1978, ni le Code de la Santé publique[65] ne définissent ces notions. En l'absence de plus de précision, ces données étaient en principe traitées comme des *« données personnelles »* bénéficiant d'un régime spécifique de protection. Intimement liées à l'individu et à sa vie privée, la loi de 1978 les qualifie de *« données sensibles »,* l'article 8 de la loi de 1978 précisant qu'il est « *interdit de collecter et de traiter des données à caractère personnel … relatives à la santé* ».

En droit communautaire, la directive 95/46 interdisait le traitement des données relatives à la santé sans mieux définir celles-ci. Mais un arrêt de la Cour de Justice de l'Union européenne du 6 novembre 2003[66] a considéré que les données de santé étaient « *des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne* », telles que l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel. Cette définition fait écho à la définition de l'OMS, selon laquelle la santé est considérée comme *« un état de bien-être physique, mental et social et ne consiste pas seulement en une absence de maladie ou d'infirmité »*[67].

L'article 4 du RGPD définit donc pour la première fois, en droit européen et dans le droit national, les données de santé : il s'agit désormais des *« données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique, y compris la prestation de soins de santé qui révèlent des informations sur l'état de santé de cette personne* ». Cette définition comprend ainsi les informations relatives à une personne physique lors d'une prestation de services de santé ou lors de son inscription en vue de bénéficier de services de soins de santé, les informations obtenues lors d'un test ou de l'examen d'une partie du corps ou encore les informations concernant une maladie, un handicap, un risque de maladie, qu'elles proviennent d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical.

Cette définition permet d'ailleurs d'englober certaines données de mesure à partir desquelles il est possible de déduire une information sur l'état de santé de la personne.

---

[65] cf. notamment les articles L. 1110-4-1 et L. 1111-8 du Code de la santé publique

[66] CJCE 6 novembre 2003, Aff.C-101/01, Linqvist, Rec.2003, I, p.12971, att n°50

[67] Préambule de la Commission de l'Organisation mondiale de la santé, New York, 19-22 juin 1946, Actes officiels de l'OMS, n°2.

Dans le contexte d'une multiplication exponentielle des données de santé, notre société est d'autant plus sensible aux problématiques d'exploitation, de fiabilité, de sécurité et de confidentialité de ce type de données, mais aussi à celles des conditions de leur valorisation.

Il est nécessaire d'abord de cerner les périmètres de la donnée de santé en tant que telle. Ensuite, il convient de caractériser les problématiques particulières de sa valorisation par l'industrie, y compris dans l'e-santé (télémédecine, actes médicaux numérisés, objets connectés), dans la mesure où des données sont utilisées pour délivrer le service aux praticiens.

3.2 Des données d'origines diverses et de valeurs différentes selon les contextes

La donnée de santé est classiquement utilisée dans trois contextes : la recherche ; la clinique ; la santé de la population en général (qui vaut pour le citoyen mais n'est pas médicale car ne génère par une décision médicale).

Comme à l'égard des données génétiques et des données biométriques, le RGPD reconnait aux États membres la possibilité de maintenir ou d'introduire des conditions supplémentaires à celles qu'il institue, y compris des limitations, en ce qui concerne le traitement des données personnelles concernant la santé. Le législateur français a fait usage de cette possibilité de déroger au RGPD. La loi Informatique et liberté donne ainsi à la CNIL le pouvoir :

- d'homologuer et de publier les méthodologies de référence destinées à favoriser la conformité des traitements de données de santé à caractère personnel ;

- d'établir et de publier des règlements types, en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données de santé ;

- de prescrire des mesures supplémentaires, notamment techniques et organisationnelles, pour le traitement des données de santé.

Un décret viendra également renforcer les conditions dans lesquelles le droit français autorise la mise en œuvre de traitement utilisant comme identifiant de santé le numéro de sécurité sociale (numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, ou NIR).

La « santé » n'a pas la même portée en droit français, dans le Code de la Santé Public ou la Loi Informatique et Liberté, où la « donnée de santé » n'est pas définie en tant que telle. Ceci est source de difficultés. La définition de « donnée sensible » du RGPD, catégorie à laquelle se rattache la donnée de santé, est très vaste, et ne tient pas compte des 3 contextes évoqués (recherche, clinique, société). Le Code de la santé publique pose certains garde-fous pour les données à usage médical, qui sont fortement protégées en France par ce code et sont placées sous le contrôle des autorités sanitaires

Une distinction de la donnée **médicale,** au sein des données de santé, associée au soin et donc nominative, apparaît comme une nécessité. Cette donnée reste personnelle au sens du RGPD, car seule la donnée individuelle intéresse le clinicien. Par ailleurs la donnée anonymisée reste porteuse de valeur pour la recherche comme pour l'entreprise.

3.2.1 La valeur pour la recherche

Les traitements de données de santé mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé sont encadrés par les dispositions du RGPD et du chapitre IX de la loi Informatique et Libertés modifiée.

Les méthodologies de référence (MR) ont été adaptées et mises à jour avec l'arrivée du RGPD. Il y a ainsi une extension à certains types de recherches dans les MR[68] :

- les recherches à risques et contraintes minimes, pour lesquelles l'information peut être collective en fonction des exigences méthodologiques de la recherche et sous réserve d'un avis favorable du CPP[69] (MR-003) ;
- la dérogation au principe du consentement écrit lors d'un examen des caractéristiques génétiques, telle que prévue à l'article L. 1131-1-1 du CSP (MR-003 et MR-004), uniquement lorsque les personnes peuvent être informées du projet de recherche et peuvent exercer un droit d'opposition. Ainsi, les cas dans lesquels l'information des personnes n'est pas envisageable et qui nécessitent donc d'obtenir l'avis d'un CPP devront faire l'objet d'une demande d'autorisation.

3.2.2 La valeur clinique, nécessairement nominative

Nous avons précisé que l'utilisation de données dans l'activité clinique, était encadrée spécifiquement (Code de la santé publique) mais cet encadrement concerne uniquement la décision médicale : une décision de type diagnostic ou une action de traitement/soin. Les données de santé sont toutes sensibles au sens du RGPD. Mais celles qui concernent la décision médicale le sont de façon particulière. En effet, c'est le rapprochement fiable de la donnée de santé avec l'identité du patient, réalisée par le praticien, qui permet à celui-ci d'établir un diagnostic.

De plus, les données de santé « appartiennent » au patient, en tout cas rien ne peut être fait sans son accord et il peut exiger de les récupérer. Pour les caractériser, il convient de s'intéresser :

- à la nature des données. Sont-elles relatives à la santé d'une personne identifiée ou identifiable ?
- à leur usage et leur finalité. Sont-elles utilisées à des fins médicales ?

Ce contexte pose problème pour l'application du RGPD : le patient à soigner ne peut rester anonyme pour le professionnel qui le prend en charge.

3.2.3 La valeur citoyenne

La donnée de santé est aussi une donnée sensible parmi d'autres, présente notamment au travers d'outils et objets du commerce, connectés ou non. La connexion confère à ces données une valeur supplémentaire car elle peut être transférée et exploitée y compris par la recherche médicale. Mais elle est aussi porteuse de risque selon la finalité des traitements auxquels elles pourront être soumis. Ce cas est typiquement celui visé par le RGPD.

---

[68] Source : https://www.cnil.fr/fr/recherches-dans-le-domaine-de-la-sante-ce-qui-change-avec-les-nouvelles-methodologies-de-reference

[69] Article L. 1122-1-4 du Code de la Santé Publique

3.3 Le RGPD, soutien de la dynamique de croissance des industries de santé

Les entreprises du secteur de la santé restent des entreprises avant tout et doivent disposer des outils adaptés pour la mise en œuvre du RGPD. Les éléments de confiance apportés par le RGPD aux entreprises qui s'y réfèrent jouent pareillement pour les entreprises de santé. Mais d'autres enjeux associés à d'autres risques, spécifiques au domaine de la santé, méritent un examen plus précis.

3.3.1 Une dynamique portée par de puissants leviers

Dans un contexte de très forte tension pour les finances publiques, il s'avère essentiel d'améliorer l'efficience et la productivité des données de santé. Dès 2014, un rapport de la CNIL soulignait que les données de santé des hôpitaux n'étaient pas valorisées. Si l'on considère la situation budgétaire, déficitaire, de la majorité des hôpitaux, cette situation ne doit pas être prolongée. En même temps, il est exclu de valoriser les données cliniques nominatives en les commercialisant en tant que telles.

Une piste est celle de la mutualisation de données entre établissements permettant ainsi d'accroitre la taille des gisements et leur potentiel de connaissances. Le secteur de la santé est en effet très en recherche d'innovations, et celles-ci sont générées par de nouvelles connaissances médicales issues des données de santé. La bonne nouvelle est que les données de santé non médicales (environnementales, comportementales) issues d'objets connectés ou d'applications de la vie courante, sont aussi porteuses de valeur, notamment quand elles sont appariées à des données médicales.

La problématique peut également se nourrir de la question de la valeur des données embarquées dans des services ou systèmes techniques à destination des praticiens. Dans tous les cas, il s'agit d'ouvrir de nouveaux marchés, de nouvelles activités économiques. Ce développement n'est pas possible sans un cadre réglementaire pertinent. Le RGPD y contribue pour une bonne part, et il appartient aux entreprises de s'en saisir

3.3.2 Une valorisation de la donnée de santé possible grâce au RGPD malgré ses limites

Les mesures réalisées par les praticiens dans l'exercice de leur activité de soin produisent des données personnelles. Mais la valeur de la donnée de santé résultant de l'activité soignante disparaît si elle est anonymisée. En effet, une donnée n'a de valeur médicale que si elle est utile aux soins, il y a donc une nécessaire identification de la personne. Cette exigence entre en tension avec les exigences du RGPD.

Or, le RGPD ne fait pas de distinction parmi les données de santé selon le risque qu'elles font courir. Ce risque peut être géré si la valeur de la donnée est réalisée dans le soin : la compétence avérée du praticien lui confère un monopole d'utilisation de ce type de donnée personnelle pour cette activité soignante. La valeur particulière de la donnée de santé pour le soin - versus pour toute autre activité même liée à la santé - nécessiterait pour cette première catégorie une désignation (donnée médicale ?) et une identification particulière.

Le statut protéiforme de la donnée de santé constitue en même temps une opportunité pour les industriels de la santé. La frontière entre données de santé et données médicales est poreuse. On constate en partant de différentes propositions de valeur d'une donnée de santé certaines posent un problème (valeur clinique nécessairement nominative), et on constate que la même donnée peut trouver sa valeur dans des domaines différents, soumis à des exigences différentes : il y a ambivalence de la donnée selon l'usage qui en est fait du fait du manque de définition. C'est typiquement le cas des données qui conditionnent la décision médicale en même temps qu'elles

constituent une source de connaissance, comme il en existe dans les cohortes de patients connectés : la remontée d'une donnée pathologique inattendue générera une mobilisation clinique.

3.3.3 Une ambivalence de la donnée de santé qui appelle la responsabilité des entreprises

Il convient sans attendre de responsabiliser les entreprises du secteur en leur permettant d'expliciter ce qui est créé comme valeur, en s'assurant que cette valorisation ne se fasse pas au détriment de la vie privée : la conjugaison entre données de santé médicales et non médicales reste en effet délicate et les entreprises devront apprendre à gérer cette situation. L'opportunité du RGPD, en l'état, est d'assouplit considérablement les contrôles sur la donnée de santé, sachant que la donnée médicale reste très encadrée.

La confiance des usagers finaux (patients) devrait s'améliorer grâce à la réaffirmation des droits des personnes que le RGPD leur confère et de la protection qu'elle leur garantit. Le RGPD mis en œuvre dans la santé permet ainsi de responsabiliser les acteurs, aussi bien les industriels que les médecins et les patients : un processus de confiance peut être engagé, qui passe par l'explicitation des règles du jeu et une clarification des usages des données.

3.3.4 L'étude d'impact, notamment, laisse aux industriels de santé le soin de définir conditions, risques et bénéfices attendus

L'analyse d'impact est à la charge du responsable de traitement. Si elle est synonyme d'une charge de travail importante, elle est toutefois totalement à la portée notamment des grandes entreprises. L'étude d'impact permet de responsabiliser les acteurs et peut constituer une réelle opportunité pour les entreprises du secteur de la santé (construire les scénarios de risque).

L'étude d'impact sur la vie privée (EIVP) s'inscrit à ce titre dans le RGPD pour la santé. C'est en effet un passage obligé pour les traitements de données personnelles porteurs de risque. Or, les traitements sur les données de santé sont à considérer, par défaut, comme « à risque ». Cette approche, est codifiée dans la loi RGPD du 20 juin 2018 et le G29 a établi des règles sur les critères de traitements à risque notamment pour l'évaluation, le croisement, l'usage innovant, la surveillance… A ce jour l'outil PIA (Privacy Impact Assessment) CNIL est le plus utilisé.

L'étude d'impact sur la vie privée vaut pour les trois périmètres des traitements en santé :

- Les traitements des données de santé comme exception à la demande d'autorisation (article 53 de la loi du 20 juin 2018) ;
- les traitements soumis à la régulation ;
- les traitements de recherche, en conformités avec les Méthodologies de référence relatives aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé.

L'étude d'impact sur la vie privée doit expliciter la légitimité de la finalité poursuivie : dans le cas de la santé, il doit déterminer le régime légal sous lequel le traitement de données à caractère personnel va être mis en œuvre.

L'étude d'impact sur la vie privée met en évidence des responsabilités partagées dans la co-conception. Des scénarios sont à élaborer, dans lesquels les événements volontaires et involontaires sur les accès, modifications et destructions de données à caractère personnel sont analysés selon la même méthode et à égalité d'importance. Les événements correspondent à des incidents techniques, des erreurs humaines, et ne concernent pas le SI.

La légitimité de l'étude d'impact, les responsabilités qu'elle souligne, par les acteurs engagés dans la conduite ou l'accompagnement de projets innovants. Ils notent toutefois un allongement et un coût significativement plus élevé pour l'étude de solutions technologiques innovantes, qui les met hors de portée d'un nombre élevé de startup et PME.

Recommandation n° 10. [CNIL] Mettre en place une qualification des prestataires qui conseillent les entreprises en matière d'impacts sur la vie privée requise pour le traitement des données sensibles, notamment de santé.

3.3.5 Toutefois, le manque de définition de la donnée de santé limite la portée du RGPD

Or, pour ce faire, il faut résoudre des problèmes liés à l'insuffisance de la définition de la donnée de santé et des différentes valeurs dont elle est porteuse.

On peut évoquer le partage de données de santé : par exemple les parcours de soin mobilisent non seulement des acteurs à l'extérieur des structures mais également des données de santé de l'hôpital, de la ville : le partage de données inter-entreprises présente des difficultés. Concernant la mise sur le marché de données entre le mains d'un industriel, qui en a fait des modèles, des bases de connaissances, issues de données fournies par l'hôpital, il y a anonymisation mais la responsabilité de l'hôpital reste entière : la donnée ne vaut que parce qu'elle permet un traitement sinon ne vaut que pour recherche.

Une meilleure définition de la donnée de santé, clarifiant les rôles et responsabilité de chacun selon les finalités qu'il poursuit est de nature à donner aux entreprises, aux startups l'opportunité de mieux s'adapter à la compétitivité industrielle, de développer de nouveaux produits, sans nécessairement supporter les exigences lourdes de la réglementation des dispositifs médicaux. Le RGPD devrait constituer alors un cadre clair permettant de s'engager dans ce type de développement. Tel est l'objet de ce chapitre.

3.4 Valoriser les données de santé : un cas d'usage

3.4.1 La valeur pour la maintenance et la traçabilité des produits de santé

La valeur pour la maintenance et la traçabilité concerne la fiabilité des équipements concernés : si la donnée est associée à l'identité d'un patient, elle devient personnelle (une défaillance de l'appareil a pour conséquence une défaillance du soin du patient). Il faut connaître l'identité du patient pour rapatrier des données utiles au clinicien ou à la vigilance sanitaire (données de maintenance mais assorties du nom du patient). La donnée de maintenance se retrouve classiquement dans les mains de l'industriel sans que l'utilisation qu'il en fait soit toujours claire (a minima, il doit pouvoir contacter le personnel traitant en cas de problème de l'équipement faisant encourir un risque ou un dommage au patient). La réglementation est à cet égard imprécise.

Recommandation n° 11. [Ministère de la Santé] Modifier le Code de la Santé Publique afin de définir les données médicales nécessitant une protection spécifique et plus forte que les autres données sensibles de santé. Par ailleurs, le droit à l'effacement ne devrait pas s'appliquer à ces données.

3.4.2 La création de valeur pour l'industrie autour de la donnée clinique

3.4.2.1 La valeur clinique d'une donnée n'existe qu'entre les mains du clinicien

Le service de soin crée de la valeur autour de la donnée de santé à condition qu'elle ne soit pas anonymisée : la donnée en elle-même est dans une relation interpersonnelle. Au-delà de la valeur médicale, la donnée qui vaut décision médicale est nécessairement non anonymisée. Il y a une forme de valorisation de la donnée par le soignant : la donnée n'a pas intrinsèquement de valeur, cette valeur résulte de l'intelligence du soignant et la donnée n'est donc qu'un élément.

3.4.2.2 La donnée clinique peut cependant s'échanger avec d'autres acteurs

Un service technique, réalisé pour le clinicien, a lui-même a besoin de personnalisation (même si la donnée technicisée est au service du soignant). Même dans le cas où des automates sont en place, ne nécessitant pas d'intervention humaine (comme par exemple la commande automatique d'une pompe à insuline suite à une analyse de glycémie) le clinicien doit en rester le garant. Ce n'est qu'à cette condition que les intérêts du patient seront préservés.

Dans le cas d'applications dans le domaine médical où le professionnel de santé n'est pas impliqué opérationnellement (exemple du pancréas artificiel) un certain nombre de questions se posent :

- Celle de la responsabilité en cas de défaillance du système technique automatisé
- Celle de la distinction entre le service fonctionnel (technique) et la prestation de soin ;
- Celle de l'anonymisation (alors que le maintien de la personnalisation peut être une condition d'efficacité du service).

Il devrait se mettre en place dans le cadre du RGPD une « responsabilité sans faute » : responsable mais pas coupable. Quand le risque n'est pas analysé, il reste un danger que l'acteur public ne peut pas traiter. L'industriel doit pouvoir faire des analyses que le monde de la santé est en droit d'exiger.

Recommandation n° 12. [Ministère de la Santé] Définir les modalités de gestion du risque associé à l'usage des dispositifs traitant des données médicales, en précisant les responsabilités réciproques du fournisseur et du ou des praticiens, au-delà du RGPD.

3.4.3 Valoriser des données anonymisées

Le Big Data représente un enjeu crucial dans la gestion et le partage des données de santé. Le rapprochement de données comportementales, environnementales et de santé permet de comprendre les conditions de diffusion du risque (et par exemple permettre des découvertes secondaires à propos de l'état de santé du patient). Il est possible pour l'industriel de santé d'accéder aux données brutes d'une base de données pour ensuite appliquer ses algorithmes. Il est évidemment nécessaire de borner ce type d'usage des données de santé, comme c'est le cas pour les données génomiques.

Différents modèles économiques sont envisageables quant à la gestion des données de santé[70] :

- Modèle free avec une base de données en accès libre pour tout acteur
- Modèle donnant-donnant : tout industriel participant à l'enrichissement de la base de données peut y avoir accès gratuitement
- Modèle de service associé aux données : les données ne sont pas accessibles pour des tiers mais des services d'analyse des données sont proposés aux industriels
- Modèle d'accès pleinement payant : si l'industriel ne participe pas à l'enrichissement de la base de données, il paie l'accès aux données (pour couvrir le coût de mise à disposition des données)

Cette gestion repose sur trois piliers : la standardisation des données de santé (format standard), la qualité des données (traçabilité et accréditations), et l'interopérabilité des données (lisibilité globale).

3.5 Cette complexité renvoie à des questions juridiques également spécifiques, parfois non résolues

3.5.1 Certaines questions spécifiques s'inscrivent dans le cadre du RGPD

3.5.1.1 La protection du citoyen-patient : articulation RGPD et Loi Informatique et Liberté

Comment cumuler les exigences de la Loi Informatique et Libertés et le RGPD en matière de santé ? La Loi Informatique et Libertés définit en effet un régime spécifique applicable aux données de santé[71] : elle s'applique lorsque les personnes concernées résident en France, même si le responsable du traitement n'est pas établi en France[72].

Les réponses diffèrent selon le cas :

- Si le traitement est hors du champ de la LIL : le RGPD s'applique seul.
- Si le traitement est dans le champ de la LIL et à d'autres fins que la recherche : il convient d'appliquer le RGPD et les articles 54 à 60 de la LIL
- Si le traitement est dans le champ de la LIL et à des fins de recherche : c'est le RGPD qui s'applique.

3.5.1.2 La matériovigilance

Récupérer des données doit permettre d'anticiper le dysfonctionnement (ou le fonctionnement normal mais qui pose problème pour le patient) et ainsi vérifier qu'il n'y ait pas d'effets secondaires, que le matériel ne génère pas de problème de santé pour le patient. Pour identifier le patient exposé au risque, il est nécessaire de rapatrier de l'information, des données déclaratives.

---

[70] Source : « Vision et propositions des industries de la santé pour le Plan France Médecine Génomique 2025 », ariis.

[71] Chap. IX, art.53

[72] Art. 5-1

3.5.2 D'autres peuvent être résolues moyennant des dispositions complémentaires

3.5.2.1 La pseudonymisation

La pseudonymisation est une anonymisation réversible. Elle s'impose en santé lorsqu'une donnée est confiée par un soignant ou un établissement de santé à un industriel pour être réutilisée par la suite – sous une autre forme. N'étant pas concerné par l'activité clinique, l'industriel ne peut traiter qu'une donnée anonyme. Mais le clinicien doit pouvoir ensuite retrouver le patient concerné.

L'industriel peut-il être considéré comme un simple sous-traitant ?

Un exemple illustrera cette question : une startup spécialisée dans l'imagerie 3D offre une prestation de modélisation singulière de l'anatomie du patient, à partir d'images médicales. Ce modèle pourrait être considéré comme une « donnée personnelle » de ce seul fait. Cette startup est un prestataire de l'hôpital. Elle ne conserve pas les données hospitalières et ne connait pas le nom de la personne dont elles sont issues. Seul un numéro aveugle est échangé, et l'entreprise ne dispose pas de donnée nominative relativement au patient. L'anonymisation est effective, qui convertit le nom du patient en un code aveugle.

Pour autant, la question de l'impact du RGPD reste posée. En effet, en cas de vente du modèle numérique, des croisements pourraient lever l'anonymat. La gestion des prospects et des clients devrait prendre en compte le risque que ce type de recoupement ait lieu. Ce cas montre les enjeux et risques associés à la sous-traitance par les établissements de santé. De fait, le RGPD doit amener les hôpitaux à s'interroger sur ce qui peut être confié aux sous-traitants et dans quelles conditions.

Le RGPD s'applique aussi bien aux collecteurs de données qu'à leurs sous-traitants. C'est de première importance dans le domaine de la santé qui centralise énormément de données dites sensibles, telles que les dossiers médicaux. Cette catégorie de données, maintenant soumise à des règles spécifiques (article 9.2), ne peut être traitée que si :

- La personne concernée a donné son consentement explicite au traitement de ses données personnelles.
- Le traitement de ces données est nécessaire à l'exécution des obligations médicales liées à l'exercice de la médecine.

Le traitement de ces données est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique. L'interprétation du RGPD confère au sous-traitant les mêmes responsabilités et obligations que l'hôpital. L'entreprise concernée devrait se doter d'un médecin hébergeur. Bien que les données soient pseudonymisées, on peut concevoir des situations où des données doivent pouvoir être détruites de façon ciblée.

La question de l'identification par rapprochement de données de sources différentes est ainsi posée. En croisant de façon massive – Big Data - de nombreuses données anonymisées, même anodines, il est possible de retrouver l'identité d'une personne. C'est une faiblesse du RGPD que de ne pas traiter cette situation. Quelles que soient les protections, des recoupements de plusieurs sources mettent en échec l'anonymisation.

La réutilisation des données à caractère personnel relatives à la santé par des opérateurs économiques comme des fabricants de produits de santé ou des organismes complémentaires d'assurance maladie doit être encadrée.

3.5.2.2 *Accéder aux données nominatives : exemple du médecin hébergeur*

Dans la cadre de l'hébergement, pour résoudre des problèmes techniques nécessitant l'accès à des données personnelles de santé, un médecin de l'hébergeur est désigné. Il serait imaginable qu'une fonction de ce type puisse jouer un rôle comparable pour des traitements personnalisés : il conviendrait donc que les prestataires manipulant des données nominatives nomment aussi un médecin. L'acte de soin prend une autre extension : il s'étend à l'acte technique qui ne peut être confié à la machine seule (le médecin est garant, avec un exercice de son métier très différent). Cet aspect a été illustré au § 3.3.3.

Toutes les entreprises traitant de données de santé personnelles sont concernées sans exception, quelles que soient ces données. Cette situation met les PME en difficulté, plus encore que dans d'autres secteurs. Au-delà du coût, la complexité réglementaire, véritable maquis, devrait voir émerger de nouvelles professions ou des professions qui étendent leurs compétences, spécifiquement dans le secteur de la santé.

L'activité d'hébergement des données de santé est très réglementée : elle doit faire l'objet d'une certification par un organisme certificateur indépendant. Les données dites de « bien-être » (nombre de pas, alimentation…), qui sont au regard du RGPD « relatives à la santé physique ou mentale d'une personne physique » donc de santé, ne sont pas soumises aux mêmes conditions de certification. Se pose donc le problème d'une évolution de la régulation des hébergeurs de données de santé.

Il y a une quantité importante d'hébergeurs agréés. Et les enjeux d'un tel agrément par rapport à l'externalisation de traitement de données personnelles risquent de stimuler encore la demande. Chacun veut être hébergeur. Un grand nombre d'hébergeurs rend difficile de suivre les croisements réalisés permettant d'identifier les personnes.

3.5.2.3 *La responsabilité médicale des traitements*

Il existe un problème de responsabilité sur le risque associé à l'équipement : une donnée identifiant le patient doit être toujours là (nominatif) mais c'est une donnée de santé, donc en principe on ne devrait pas y avoir accès. On engage la responsabilité de l'industriel mais on ne dégage pas responsabilité du praticien.

Recommandation n° 13. [Ministère de la Santé] Mettre en place un groupe de travail en lien avec le Health Data Hub afin de prendre des mesures de prévention des risques de désanonymisation résultant de croisements de données anonymisées et ou pseudonymisées pouvant déboucher sur des atteintes à la vie privée.- par exemple par la définition du rôle de médecins de type « médecin de l'hébergeur », habilités à accéder aux données de santé.

3.5.3 D'autres enfin nécessitent de nouvelles règles

3.5.3.1 *Une nécessaire clarification de la donnée de santé et des textes auxquels se référer (Code de la Santé Publique versus RGPD)*

Des données deviennent des données de santé :

- En cas de croisement des données qui permet une conclusion sur un état de santé ou un risque pour la santé (par exemple le croisement entre la tension et la mesure de l'effort).

- Selon la destination des données (destination au plan médical). Ne faudrait-il pas «restreindre» la surface de la donnée de santé pour assurer la sécurité des personnes ?

La subsidiarité des Etats membres sur certaines données sensibles[73] implique une gestion des différences éventuelles entre des états, ainsi que la maîtrise des réglementations spécifiques dans chaque état membre de l'UE. A quel point cela est-ce possible ?

Lorsqu'ils sont conformes à des référentiels établis par la CNIL, ces traitements peuvent être mis en œuvre à la condition que leurs responsables adressent préalablement à la CNIL une déclaration attestant de leur conformité. La CNIL peut autoriser par une décision unique plusieurs traitements similaires. Pour les traitements contenant des données de santé justifiés par une finalité d'intérêt public, la nouvelle loi prévoit que la CNIL en concertation avec l'Institut national des données de santé puisse adopter des règlements types et des méthodologies de référence qui constitueront la règle. Ainsi, même en matière de santé les autorisations de la CNIL seront l'exception.

3.5.4 Cette création de nouvelles règles peut échapper au droit positif

La nécessité de créer de nouvelles règles peut passer par la mise en place de codes de bonne conduite, les référentiels (façons d'agir : on sort du domaine du droit pour entrer dans celui de la déontologie) et les normes ISO.

Le RGPD favorise la co-conception, non pas nécessairement dans une approche de droit classique, d'une juridiction, mais dans une approche horizontale avec une concertation et une collaboration des acteurs. Cette approche de co-construction est d'autant plus pertinente que le secteur de la santé est très évolutif Ainsi, l'une des pistes développées par le RGPD est qu'il faut privilégier une approche contractuelle plutôt que par le droit, avec le risque d'avoir autant d'approches contractuelles que de situations. Le RGPD est un véritable facteur de revitalisation du secteur de la santé (il peut permettre une restructuration des entreprises du secteur). Il s'agit en tous cas d'une opportunité pour les industriels: il leur appartient de s'en saisir et de s'organiser à cette fin.

3.6 Conclusion

Le RGPD est vecteur de trois idées fortes :

- Un assouplissement de la législation
- Une circulation des données facilitée
- Une responsabilisation des acteurs.

Ce nouveau contexte est favorable à la numérisation du secteur et devrait permettre le développement des industries de santé. Mais pour cela, il est nécessaire que les acteurs économiques s'en saisissent et s'organisent. Ceci suppose le développement d'interactions multilatérales, horizontales (l'échange de données passe par une interopérabilité généralisée), une collaboration accrue entre entreprises, avec sans doute l'émergence de nouvelles professions.

La législation pose un cadre qui apparait réfléchi et pertinent. Il laisse aux Etat membres une marge de manœuvre pour s'organiser. Mais industriels ont aussi des choix à faire pour s'organiser. Dans le cadre de la démocratie sanitaire, c'est l'affaire pas seulement de l'Etat mais aussi des acteurs industriels.

[73] Article 9.4 du RGPD

4 LA MISE EN ŒUVRE DU RGPD DANS LES SERVICES FINANCIERS

L'examen de la mise en œuvre du règlement général sur la protection des données personnelles à travers son impact sur les services financiers présente un intérêt à plusieurs titres.

En premier lieu, les services financiers destinés aux particuliers reposent essentiellement sur le traitement de données à caractère personnel et illustrent bien tous les aspects de la définition qu'en donne le règlement : « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* » [74].

En second lieu, les services financiers sont très encadrés. La plupart des acteurs sont soumis à un agrément délivré par les autorités prudentielles et sont soumis à la surveillance de ces autorités : l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) et l'Autorité des Marchés Financiers (AMF) en France. Les règles qui s'appliquent aux établissements financiers trouvent pour la plupart leur origine dans le droit communautaire. Le système du « passeport européen » permet assez facilement à un acteur du marché d'exercer ses activités dans d'autres Etats membres que le sien. Ainsi, le secteur financier est pleinement en situation de bénéficier du surcroît d'harmonisation européenne induit par le RGPD en matière d'utilisation des données personnelles[75].

4.1 Les travaux de mise en conformité

Alors que les entreprises du secteur financier étaient à l'évidence très concernées par la mise en œuvre du RGPD et que celui-ci a été publié au Journal Officiel de l'Union Européenne dès le 4 mai 2016, les travaux de mise en conformité semblent en général avoir été engagés tardivement. Ce n'est ainsi qu'en octobre 2017 que, parmi les premiers, la Société Générale communique sur la désignation d'un « *data protection officer* ».

A la décharge des acteurs, une abrogation plus diligente, à effet du 25 mai 2018, des dispositions de la loi de 1978[76] contraires au RGPD, ainsi qu'une plus grande clarté des dispositions résiduelles applicables en France, auraient sans doute été propices à une mise en œuvre ordonnée du règlement[77].

Le profil des *data protection officers* désignés par les différents établissements financiers apparaît extrêmement variable : les fonctions qu'ils exerçaient précédemment sont, selon les cas, des fonctions juridiques, commerciales, informatiques ou stratégiques. Cette diversité illustre bien la variété des réflexions engendrées par la mise en œuvre du RGPD.

---

[74] Article 4-2) du règlement

[75] On vise ici tout particulièrement le recours au règlement et l'abrogation des règles antérieures édictées sous la forme de directives (directive 95/46/CE), ainsi que la subordination de la CNIL à un comité européen de la protection des données

[76] Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

[77] La mise en cohérence du droit français avec le RGPD a été engagée à contretemps par la loi n° 2018-493 du 20 juin 2018 et complétée par l'ordonnance n°2018-1125 du 12 décembre 2018

Les établissements rencontrés portent en général une appréciation positive sur le RGPD : la confiance de la clientèle est essentielle à leurs activités et une bonne conformité aux obligations posées par le règlement est volontiers incorporée à leur stratégie de communication. Pour les établissements ayant des succursales dans d'autres pays européens, une réglementation commune en matière de protection des données personnelles permet de standardiser certaines règles internes. L'importance de la charge de mise en conformité est relevée par tous les acteurs, qu'il s'agisse d'acteurs historiques dont les systèmes d'information sont mal urbanisés ou d'acteurs récents qui ont peiné à constituer une équipe dévolue à ce projet. Il ne semble pas que les acteurs récents aient disposé d'un avantage compétitif ; à la différence de futurs établissements financiers qui intègreraient dès leur conception les obligations du RGPD (le « *privacy by design* »).

Les opportunités de développement offertes par le RGPD sont mal identifiées. Alors que le régime d'autorisation ou de déclaration préalable institué par la loi de 1978 était objectivement très contraignant, la responsabilisation des acteurs et la plus grande flexibilité dont ils peuvent bénéficier dans le cadre du RGPD semblent encore les effrayer. En fait, la mise en place du RGPD a eu pour effet immédiat de réévaluer sensiblement la perception par les entreprises des enjeux de données personnelles.

4.2 Les interactions entre le RGPD et la DSP2

Pour beaucoup d'acteurs des services financiers, le RGPD a eu moins d'impacts que la seconde directive sur les services de paiement (DSP2) [78], publiée le 23 décembre 2015 et entrée en vigueur le 13 janvier 2018, ainsi que la directive déléguée[79] qui en précise les mesures d'application, publiée le 13 mars 2018 et applicable le 14 septembre 2019. Mais la mise en œuvre concomitante de ces deux textes, qui présentent quelques interdépendances, a été parfois difficile à mener dans le même calendrier.

L'une des dispositions les plus commentées de la DSP2 consiste en une obligation faite aux banques et aux autres établissements teneurs de comptes de paiement de permettre à des établissements tiers faiblement régulés (« agrégateurs de comptes » ou « initiateurs de paiements ») d'accéder gratuitement aux relevés des comptes de paiement, sur simple autorisation de leurs clients communs. La directive déléguée invite les banques à faciliter et à sécuriser ces échanges par la mise en œuvre d'API (*application programming interface*).

Il existe manifestement une communauté de finalité entre le droit à la portabilité des données, disposition à caractère général prévue à l'article 20 du RGPD, et l'obligation faite spécifiquement aux banques par la DSP2 de faciliter l'accès aux données de leurs clients. Dans les deux cas, l'intention du législateur européen consiste à renforcer la concurrence au bénéfice du consommateur, en limitant les barrières à l'entrée et les situations acquises. Mais le droit à la portabilité prévu par le RGPD n'est pas encadré par un délai : rien n'interdit que sa mise en œuvre prenne plusieurs jours. La confection

[78] Directive 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE

[79] Règlement Délégué 2018/389 de la Commission du 27 novembre 2017 complétant la directive 2015/2366 par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication

et la mise à disposition gratuite d'API dans le cas des prestataires de services de paiement présentent un niveau d'exigence considérablement plus élevé, sans que l'importance de cet écart soit bien motivée.

L'article 97 du RGPD invite la Commission, au plus tard le 25 mai 2020, à établir un rapport public sur l'évaluation et l'opportunité de faire évoluer le règlement. S'agissant de la DSP2, c'est au plus tard le 13 janvier 2021 que la Commission doit établir un rapport sur l'application et sur l'impact de la directive, éventuellement assorti d'une nouvelle proposition législative[80]. Dans cette perspective, il semblerait opportun d'élaborer une doctrine tendant à justifier par un soubassement théorique l'existence de règles aussi divergentes entre les services de paiement et les autres services aux particuliers.

On pourrait à cette occasion examiner l'intérêt qu'il y aurait à renforcer le droit à la portabilité (en imposant par exemple une mise en œuvre en temps réel ou des conditions d'authentification du demandeur) ou à étendre à d'autres services que les services de paiement l'obligation de mettre gratuitement à la disposition d'un tiers désigné par un client les données de celui-ci (autres services financiers, services de transport, constructeurs automobiles, services de santé, etc.)

4.3 Les relations entre donneurs d'ordre et sous-traitants

Le chapitre IV du RGPD est consacré aux relations entre le responsable d'un traitement mettant en jeu des données personnelles et son sous-traitant. L'article 28 tend à affirmer la prééminence de la responsabilité du responsable du traitement et à encadrer fermement l'action du sous-traitant : le sous-traitant doit présenter des garanties suffisantes, de manière à ce que le traitement qu'il effectue garantisse la protection des droits personnels ; le sous-traitant ne doit pas recruter un autre sous-traitant sans l'autorisation écrite préalable du responsable du traitement ; le traitement par un sous-traitant doit être régi par un contrat prévoyant notamment qu'il ne traite des données à caractère personnel que sur instruction documentée du responsable du traitement, etc.

La renégociation des contrats en cours a souvent constitué un enjeu majeur de mise en conformité des entreprises financières avec le RGPD. Evidemment, chaque fois qu'il a été question de renforcer les obligations d'un sous-traitant, celui-ci pouvait s'estimer fonder à négocier des contreparties, notamment financières. Lorsque la puissance de négociation du sous-traitant était plus importante que celle du donneur d'ordre, ou lorsque le sous-traitant n'était pas établi dans un Etat membre de l'Union européenne (mais par exemple aux Etats-Unis ou en Chine), les discussions ont pu être âpres.

En pratique, il a pu sembler plus commode, parfois, de présenter les relations entre deux entreprises, vis-à-vis d'un traitement donné, comme des relations de responsables conjoints de ce traitement au sens de l'article 26 du RGPD : « *lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD* ». On peut se demander si ce choix ne risque pas de vider l'article 28 d'une partie de sa substance et, dans certains cas, de conduire à une certaine dilution des responsabilités de l'établissement financier donneur d'ordres.

[80] Article 108 de la DSP2

Ainsi, un arrêt récent de la Cour de Justice de l'Union européenne[81], dans un contexte pré-RGPD, illustre bien les questions de responsabilité soulevées par la sous-traitance : il s'agissait de déterminer si l'ULD, homologue de la CNIL dans le Land du Schleswig-Holstein, avait à bon droit pu ordonner à la Wirtschaftsakademie, qui offre des services de formation, de désactiver la page fan qu'elle avait créée sur Facebook, au motif que ni la Wirtschaftsakademie ni Facebook n'informaient les visiteurs de la page fan que ce dernier collectait, à l'aide de cookies, des informations à caractère personnel les concernant et qu'ils traitaient ensuite ces informations.

Au demeurant, en droit français, parmi le vaste ensemble de dispositions qui régissent le contrôle interne des établissements financiers[82], des règles particulières visent la situation où « *les entreprises assujetties externalisent des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes* ». Elles visent à ce que les entreprises assujetties demeurent pleinement responsables du respect de toutes les obligations qui leur incombent et, plus particulièrement, à ce que les relations de l'entreprise assujettie avec ses clients et ses obligations envers ceux-ci n'en soient pas modifiées, à ce que l'entreprise assujettie contrôle effectivement les prestations ou les tâches externalisées et gère pleinement les risques associés à l'externalisation.

Compte tenu de la difficulté qu'ont eu les entreprises à traduire contractuellement dans un temps réduit les dispositions du RGPD relatives à leurs relations avec des sous-traitants, compte tenu de la diversité des entreprises financières (en termes de taille, d'organisation juridique et de pays d'établissement), compte tenu enfin de la puissance de négociation de certains sous-traitants (s'agissant par exemple de la fourniture de services d'hébergement de données et de programmes sur le cloud), il peut sembler utile, quelques mois après la mise en œuvre du RGPD, de s'assurer de l'homogénéité des solutions retenues en termes de protection et de sécurité des données personnelles.

4.4 La coopération entre l'ACPR et la CNIL

L'ACPR est l'autorité chargée de veiller à la préservation de la stabilité du système financier et à la protection des clients, assurés, adhérents et bénéficiaires des entreprises soumises à son contrôle[83], parmi lesquelles figurent les établissements de crédit, les entreprises d'investissement, les établissements de paiement, les prestataires de services d'information sur les comptes (agrégateurs), les établissements de monnaie électronique... L'ACPR contrôle le respect par ces établissements financiers des règles qui leur sont spécifiquement applicables.

Parallèlement aux responsabilités de contrôle prudentiel qui lui incombent au titre des directives européennes, l'ACPR est chargée de veiller au respect par les personnes soumises à son contrôle des règles destinées à assurer la protection de leur clientèle, ainsi qu'à l'adéquation des moyens et

[81] Arrêt de la Cour du 5 juin 2018 dans l'affaire C‑210/16, répondant à une demande de décision préjudicielle dans la procédure ULD Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH, en présence de Facebook Ireland Ltd

[82] Arrêté du 3 novembre 2014 modifié relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution, cf. en particulier Titre V : les systèmes de surveillance et de maîtrise des risques, chapitre II : Conditions applicables en matière d'externalisation

[83] Article L. 612-1 et suivants du Code monétaire et financier

procédures que ces personnes mettent en œuvre à cet effet : c'est le rôle, au sein de l'ACPR, de la Direction du Contrôle des Pratiques Commerciales. Pour l'accomplissement de l'ensemble de ses missions, l'ACPR dispose d'un pouvoir de contrôle sur pièces et sur place, du pouvoir de prendre des mesures de police administrative et d'un pouvoir de sanction.

L'article L. 631-1 du Code monétaire et financier organise la levée du secret professionnel entre la Banque de France, l'ACPR, l'AMF et d'autres institutions dont les prérogatives sont voisines : le Haut Conseil du commissariat aux comptes, des fonds de garantie tels que le fonds de garantie des dépôts et de résolution… peuvent ainsi coopérer en se communiquent les renseignements utiles à l'accomplissement de leurs missions respectives. Il en va de même avec l'autorité administrative chargée de la concurrence et de la consommation – mais pas avec la CNIL.

On ne voit pas bien pourtant comment on pourrait dissocier de la protection du consommateur, au sens où l'entend l'ACPR, la protection de ses données personnelles : pour prendre un exemple, la confidentialité des identifiants bancaires, qui permettent aux consommateurs d'accéder à leurs sites de banque en ligne et de procéder à des virements au profit de tiers, est à l'évidence un enjeu majeur commun à l'ACPR et à la CNIL. Il apparaît dès lors indispensable que les textes prévoient et encadrent les modalités de coopération entre ces deux institutions.

Recommandation n° 14. [Direction générale du Trésor] Préciser au paragraphe II.3° de l'article L. 612-1 du Code Monétaire et Financier que la protection des données personnelles de la clientèle des établissements financiers entre dans le champ de contrôle de l'ACPR et prévoir par une disposition de ce code que l'ACPR et la CNIL doivent coopérer et peuvent se communiquer les renseignements utiles à l'accomplissement de leurs missions respectives

5 QUELLES NOUVELLES ACTIVITES ECONOMIQUES APPARAISSENT ?

La protection des données personnelles étant un sujet sensible pour le grand public, le RGPD peut être un argument marketing, et plus généralement peut contribuer à rétablir la confiance des citoyens envers les entreprises. Par exemple, Qwant, le moteur de recherche français, fait savoir qu'il est plus protecteur de la vie privée que d'autres moteurs de recherche. Cependant, sur le marché européen, une entreprise n'a pas d'avantage compétitif en se conformant au RGPD, puisque ses concurrentes doivent aussi le faire, qu'elles soient de droit européen ou non[84].

On pourrait imaginer que les entreprises européennes cherchent à profiter, sur les marchés non européens, de leur expérience en matière de protection de données personnelles acquises grâce au RGPD et demandent à leurs filiales non européennes d'appliquer le RGPD : elles pourraient alors légitimement affirmer qu'elles font le plus grand cas de la protection de la vie privée de leurs clients. Or, il semble qu'il n'en est rien dans les domaines de la finance et de la santé. La quasi-totalité des entreprises interrogées par la mission, qui ont des activités hors Europe, ont fait le choix de ne déployer le RGPD qu'en Europe. Les mêmes assurent cependant qu'un droit commun aux pays européens en matière de protection des données personnelles facilite les échanges de données entre les entités de différents pays européens, et cet argument semble pouvoir s'appliquer à leurs activités hors Europe. Les raisons avancées par les entreprises sont (1) l'investissement nécessaire pour passer au RGPD est élevé (de l'ordre d'une centaine de millions d'euros pour un grand établissement financier, par exemple) (2) les pays non européens peuvent à l'avenir adopter une réglementation différente du RGPD, ce qui obligera les filiales non européennes à s'adapter deux fois.

Les jeunes entreprises, qui sont « RGPD by design », si elles se conforment bien dès leur naissance à la réglementation, sont, en première analyse, celles qui bénéficieront de l'avantage compétitif d'une meilleure protection des données personnelles sur les marchés non européens, puisqu'elles n'auront pas cette barrière à l'entrée qui représente la conversion d'un système de gestion de données à un autre. Plus généralement, des entreprises européennes du numérique y trouveront un avantage compétitif sur les marchés extra-européens[85].

Même de si prime abord le RGPD peut paraître principalement contraignant, sa philosophie générale implique notamment de mener une analyse d'impact relative à la protection des données. Ces analyses d'impact sont loin d'être superflues compte tenu des cyber-attaques visibles (destruction de données, indisponibilité des SI…) ou invisibles (vol de données, espionnage économique…). Elles ont en effet le mérite d'obliger les entreprises à inventorier leur patrimoine immatériel constitué de données, à analyser les risques encourus et à dresser une liste des mesures de protection matérielles, logicielles ou organisationnelles.

Si les plus grandes entreprises se sont appropriées ces bonnes pratiques en matière de protection des SI, il n'en va pas forcément de même pour les PME et les TPE. Pour ces dernières, les méthodes[86] et l'accompagnement[87] existent, permettant ainsi aux plus petites entreprises de retenir des

---

[84] Ainsi les arguments de Qwant en matière de protection de la vie privée deviennent peu audibles lorsque tous les moteurs de recherche, y compris non européens, affirment être compatibles avec le RGPD.

[85] Source DGE

[86] Guide des bonnes pratiques de l'informatique CPME - ANSSI

[87] Par ex. le Conseil Supérieur de l'Ordre des Experts-Comptables

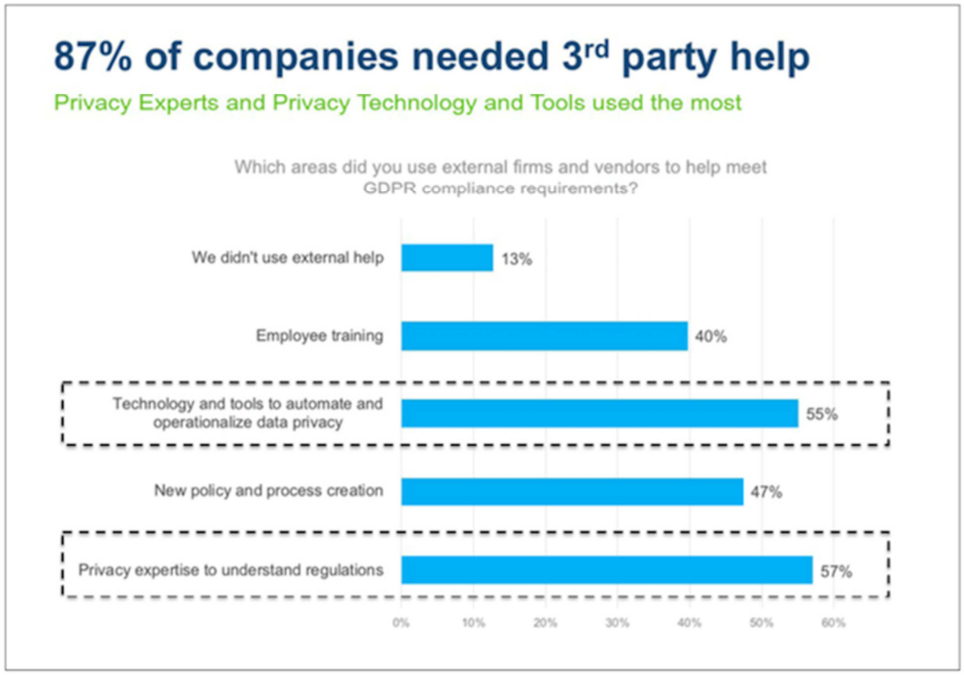
solutions adaptées et proportionnées à leurs besoins parmi la liste des produits et services qualifiés par l'ANSSI.

Cependant, des activités économiques émergentes de trois types peuvent être favorisées par la mise en place du RGPD : (1) celles nécessitées par la stricte mise en place de ce règlement dans les entreprises (2) les services et les logiciels qui facilitent ou automatisent l'application des nouvelles règles (3) les standards, labels, et certifications associés.

Le DGE estime les marchés supplémentaires générés par le RGPD à environ 1 Mds€/an.

5.1 Certaines activités existent en accompagnement du RGPD

De nombreuses entreprises ont cherché à répondre aux besoins d'assistance pour se conformer au RGPD, au point que la CNIL et la DGCCRF ont dû alerter sur des pratiques abusives (tarifs prohibitifs, collecte d'informations en vue d'une escroquerie ou d'une attaque informatique). Ces activités économiques nouvelles créent potentiellement des emplois mais ont un coût pour les entreprises existantes. Ce sont des services de proximité, qui ont peu ou pas de potentiel d'exportation. « Près de 87% des entreprises ont éprouvé le besoin de faire appel à une aide extérieure, expertise sur le domaine juridique, technologique, ou outils pour automatiser et rendre opérationnelle la gestion des données personnelles »[88] comme l'illustre le diagramme ci-dessous.



5.1.1 Les conseils juridiques et informatiques

De nombreux cabinets juridiques, et sociétés informatiques, proposent leurs services, notamment à des PME ne disposant pas des compétences nécessaires. A noter que l'article 35 du RGPD impose des analyses d'impact relatives à la protection des données personnelles dans des cas précis comme la « surveillance systématique à grande échelle d'une zone accessible au grand public ». Les éditeurs de

[88] https://itsocial.fr/enjeux/securite-dsi/reglementation/cout-de-conformite-rgpd/

logiciels, ou d'autres entreprises, devront aider à la réalisation de ces analyses d'impact, le cas échéant.

5.1.2 La mutualisation des DPO

Des PME, et des collectivités locales peuvent avoir intérêt à mutualiser ce service de DPO, pour avoir accès à une compétence juridique de qualité à moindre coût. L'offre actuelle présente une grande disparité en termes de prix et de qualité, d'après la CNIL. Une certification devrait être mise en place (voir ci-dessous §3.2).

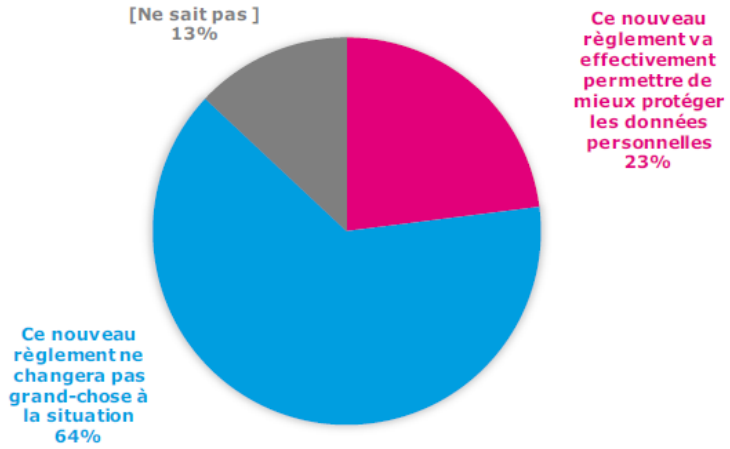
5.1.3 Les formations et la sensibilisation au RGPD

Certaines entreprises ont l'impression que les utilisateurs ne sont pas forcément éduqués aux bénéfices du RGPD. Le manque de sensibilisation des clients ne permet pas de jouir d'un levier de business. Une campagne nationale qui explique la démarche RGPD et valorise les entreprises qui respectent le règlement pourrait être un moyen de changer cela. Le diagramme ci-dessous[89] illustre la faible proportion de citoyens estimant que le RGPD est un réel changement bénéfique pour la protection des données à caractère personnel.

Un peu moins d'une personne sur quatre est convaincue de l'efficacité du RGPD

Graphique 100 – En mai 2018, un nouveau règlement européen est entré en vigueur, afin de renforcer le contrôle des citoyens sur l'utilisation de leurs données personnelles. A ce sujet, diriez-vous plutôt ?

- Champ : ensemble de la population de 12 ans et plus, en % -



Source : CREDOC, Enquête sur les « Conditions de vie et les Aspirations », juin 2018.

Plusieurs types d'actions sont proposées comme des formations intra ou interentreprises, des MOOC pour se familiariser au RGPD (CNAM, Rue de la formation) etc. Par ailleurs, des packs de conformité par secteur d'activité sont progressivement publiés. Cette activité économique, sans doute limitée dans le temps à la mise en conformité RGPD des entreprises, est en « coopétition » avec les guides pratiques disponibles sur les sites de la CNIL, Bpifrance, CIGREF, AFAI[90] etc…

[89] Source : baromètre du numérique CGE-ARCEP-Agence du numérique 2018

[90] Association française de l'audit et du conseil informatiques

5.2 Mais le RGPD permet aussi le développement de nouvelles activités

5.2.1 La sécurisation des données

L'article 32 du RGPD fait obligation au responsable de traitement (et le sous-traitant) de mettre en œuvre « les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ». Il faut souligner que le RGPD introduit une notion de conformité dynamique dans le temps : le responsable de traitement ne doit pas se conformer à cette obligation de sécurité « appropriée » uniquement le 25 mai 2018 mais en permanence : cela crée une activité réelle sur le long terme. La spécificité du RGPD est qu'il s'applique à toutes les entreprises dès lors qu'elles traitent de la donnée personnelle, créant une obligation de sécurité, avec possibilité de sanction, ce qui permet d'élever le niveau de cybersécurité. Les entreprises qui offrent des conseils, des formations ou des solutions de cybersécurité sont ainsi encouragées.

Or, la France dispose de très bonnes compétences scientifiques en cybersécurité, notamment en matière de cryptologie des algorithmes et des protocoles, et de méthodes formelles ; les équipes de l'Institut Mines Télécom sont très actives aux côtés de l'INRIA, du CEA, du CNRS, des écoles du Ministère des Armées, et de l'ANSSI. Le secteur industriel de la cybersécurité représente environ 6 Md€/an avec des acteurs de premiers plans comme Thalès, et une croissance de 12 % par an, sur les 5 dernières années. Le Comité de la filière industrielle de la sécurité a été transformé fin 2018 en Comité stratégique de filière au sein du CNI. La sécurité des données est un enjeu essentiel pour les entreprises qui offrent des solutions de type « Cloud », ou des data centers (OVH…). En effet, toute la chaîne des acteurs, y compris les sous-traitants sont co-responsables de la protection des données selon le RGPD.

Le secteur de la cybersécurité, bien antérieur au RGPD, peut y trouver l'occasion de développer de nouveaux produits, spécifiques à la protection des données personnelles.

5.2.2 L'anonymisation des données à caractère personnel

La pseudonymisation[91] des données est, au même titre que le chiffrement, une méthode pour garantir un niveau de sécurité approprié (article 32 du RGPD) ; elle n'est pas considérée ici, car elle relève du paragraphe précédent. L'anonymisation des données personnelles permet de sortir du champ d'application du RGPD[92] : ainsi, à l'issue du traitement des données, ou si une personne exerce son droit à l'oubli, l'anonymisation peut être une alternative à l'effacement. La personne concernée ne doit plus être identifiable, par quelque moyen que ce soit ; c'est-à-dire aucune donnée ou ensemble de données ne permet plus de retrouver son identité. Des logiciels existent d'ores et déjà : IBM, Informatica, et Oracle assuraient 75 % du marché du data masking en 2015, selon une étude de Gartner[93] ; les 11 autres, la plupart américaines, les 25% restants. Les enjeux de l'anonymisation sont considérables : l'économie de la donnée se développera surtout sur des données « communicables », c'est-à-dire non soumises au RGPD. Par exemple la grande distribution a pris conscience que les données personnelles qu'elle détenait représente une valeur importante dont elle peut tirer parti, à condition de les anonymiser.

---

[91] La pseudonymisation consiste à scinder de manière réversible les données identifiantes des autres données, par exemple, remplacer un nom par des chaînes de caractère.

[92] Considérant 26 du préambule.

[93] Magic Quadrant for data masking technology, worldwide.

L'anonymisation est une alternative à la suppression définitive des données. Ces données, n'étant dès lors plus des données à caractère personnel, peuvent être conservées librement et valorisées notamment par la production de statistiques[94]. **Le processus d'anonymisation est actuellement très coûteux et offre certainement des perspectives de développement suite à la mise en place du RGPD.**

Des éditeurs français peuvent chercher à profiter de la mise en place du nouveau règlement européen ; compte-tenu de la concurrence, ils devraient le faire sur un secteur émergent. Le risque de ré-identification est la principale menace qui pèse sur tout projet ou tout logiciel d'anonymisation. Un des enjeux est de mettre au point des méthodes ou des algorithmes pour évaluer ce risque. C'est ce que font des instituts de recherche comme Télécom Sud Paris, et des entreprises.

Malgré l'anonymisation, il est possible dans certains cas de reconstituer des données d'identification grâce au recoupement de plusieurs données prétendument anonymisées. Les données considérées sont donc en réalité des données indirectement personnelles, qui restent soumises au RGPD[95]. Il y a donc également un enjeu d'évaluation des procédés et de leur efficacité.

La CNIL a la possibilité de certifier les solutions d'anonymisation, ou les entreprises dont les processus mis en place permettent de garantir l'anonymisation, depuis la Loi pour une République numérique du 7/10/2016 (voir §3).

5.2.3 La création de bases de données d'intérêt général ou « hub de données »

Cette activité n'est pas « issue » de la directive européenne, et les éventuelles données personnelles devraient y être anonymisées.

5.2.4 L'automatisation de la collecte des données et de la suppression des données

Des logiciels ou des processus innovants peuvent sans doute être développés.

Recommandation n° 15. [Bpifrance, DGE] Lancer des appels d'offres pour des travaux de R&D et de logiciels prototypes en matière de suppression automatique de données, d'anonymisation des données, et d'évaluation du risque de ré-identification, par exemple dans le cadre du plan IA.

5.3 Standards, labels et certifications

5.3.1 Les standards de portabilité

La portabilité est un nouveau droit introduit par le RGPD. Mais comment assurer le transfert des données d'une banque à une autre par exemple ? Des standards devront être mis en place, sans

[94] Article 26 du RGPD

[95] Pour mesurer l'efficacité de l'anonymisation de données, le G29 (Avis 05/2014 sur les techniques d'anonymisation du Groupe de travail Article 29 sur la protection des données) propose notamment trois critères cumulatifs permettant d'apprécier l'efficacité d'une technique d'anonymisation : l'individualisation (possibilité d'isoler une partie ou la totalité des informations identifiant une personne dans un ensemble de données), la corrélation (possibilité de relier entre elles au moins deux informations se rapportant à la même personne ou au même groupe) et l'inférence (capacité de déduire la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs).

doute par secteurs industriels. Google et Microsoft, notamment, proposent déjà des outils, mais une offre française est sans doute possible dans les domaines non encore couverts.

5.3.2 Certifications et accréditations

Selon l'article 43 du RGPD, les organismes de certification, qui délivrent les certificats à des opérations de traitement, sont accrédités par la CNIL, ou par le COFRAC[96]. D'après l'article 42 du RGPD, la certification est volontaire et ne diminue pas la responsabilité du responsable de traitement ou son sous-traitant ; la certification est délivrée pour une durée maximale de 3 ans.

La certification permet au client (entreprise ou particulier) d'avoir une confiance accrue dans le service auquel il accède ou le produit qu'il achète puisque les opérations de traitement correspondantes sont certifiées conformes au RGPD.

Les organismes de certification représentent en eux-mêmes une activité économique qu'il faut développer plus volontairement.

Recommandation n° 16. [CNIL] Mettre en place une politique de certification RGPD de traitements et de labélisation de prestataires s'appuyant sur une méthode d'évaluation et la mise en place d'organismes de certification sur le modèle de la procédure de l'ANSSI pour les produits et prestataires de cyber-sécurité.

[96] Comité français d'accréditation

ANNEXES

Annexe 1 : Lettre de mission

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES
TELEDOC 792
BATIMENT NECKER
120, RUE DE BERCY
75572 PARIS CEDEX 12

Affaire suivie par : Benoît LEGAIT
Téléphone : 01 53 18 54 71
Télécopie : 01 53 18 57 15
Mél. : benoit.legait@finances.gouv.fr
N° 427

Paris, le 9 avril 2018

Le Vice-président

à

Philippe Louviau
Robert Picard
Maurice Sportiche
Rémi Steiner

Objet : Thème d'approfondissement de la section Technologie et Société

La confiance dans le numérique s'est construite en France sur un cadre législatif exigeant en matière de protection des données personnelles. Le socle en a été la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi a accordé une protection élevée aux données à caractère personnel et a soumis, sous le contrôle de la CNIL, les traitements afférents à ces données à des régimes de déclaration et d'autorisation a priori.

L'objectif du marché unique européen a conduit la commission à harmoniser progressivement les règles applicables dans les Etats membres en la matière, notamment à travers la directive 95/46/CE sur la protection des données personnelles.

Plus récemment, le règlement 2016/679 du 27 avril 2016 relatif à la « protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » (RGPD), applicable de plein droit dans l'Union européenne dès le 25 mai 2018, a introduit en France des droits nouveaux pour les personnes (droit à l'accès, à l'oubli, à la portabilité…) ; l'autorégulation des acteurs remplace le contrôle a priori, en vigueur jusque-là en France en matière de protection des données personnelles.

Le projet de loi relatif à la protection des données personnelles modifie ainsi des pans entiers de la loi de 1978. La CNIL est désormais affiliée à un dispositif paneuropéen de contrôle du bon usage des données personnelles. Les régimes de déclaration et d'autorisation des traitements informatiques sont abrogés.

L'Europe a fait le choix d'un haut standard de protection des données, qui devrait renforcer la confiance des individus, consolider l'écosystème numérique européen, et favoriser les entreprises du numérique. Néanmoins, les enjeux apparaissent particulièrement importants pour deux types d'entreprises :

- Les entreprises qui développent des innovations fondées sur l'exploitation de données personnelles peuvent être confrontées à des incertitudes quant à la compatibilité de leurs activités avec le RGPD, qui offre plus de flexibilité et tend à

une harmonisation européenne mais prévoit des sanctions bien supérieures à celles des réglementations antérieures. Par exemple, elles devront recueillir l'accord des personnes concernées pour tout traitement ayant une ou plusieurs finalités spécifiques. Les exigences portant sur les données personnelles sont susceptibles d'alourdir et de ralentir le processus d'innovation, menaçant de ce fait la compétitivité des entreprises ;

- Même si les PME sont dispensées de certaines obligations, comme la désignation d'un délégué à la protection des données, la consignation de leurs activités de traitement, ou l'analyse d'impact, ces assouplissements sont assortis de conditions restrictives qui en limitent la portée. Par ailleurs, les PME doivent respecter le droit des personnes, de transparence et de sécurité du traitement pour les données qu'elles traitent, a minima de ressources humaines ; or, elles disposent souvent de compétences limitées pour opérer cette transformation et la nouveauté de la réglementation fait obstacle à un partage des meilleures pratiques.

En s'appuyant sur les secteurs de la banque/assurance et de la santé, pour lesquels la protection des données personnelles est particulièrement sensible, la mission s'attachera, pour les entreprises développant des innovations qui font appel à des données personnelles, et pour les PME, à :

- ✓ formuler des recommandations d'action des pouvoirs publics, notamment en termes d'accompagnement, pour que ces entreprises tirent le meilleur profit du RGPD.

Vos travaux pourront s'appuyer sur une cartographie des risques et des opportunités de la mise en place du RGPD, notamment sur le plan sociétal.

Je vous désigne, sur proposition du président de la section Technologie et Société, rapporteurs de cette mission.

En termes de méthode :

- vous prendrez l'attache des administrations concernées (DGE, DINSIC…), des autorités administratives (CNIL….), et d'acteurs privés ;
- vous formulerez des propositions concrètes et opérationnelles à destination des ministres chargés de l'économie et du numérique, en mettant l'accent sur les outils à la disposition de la puissance publique ;
- vous rendrez compte périodiquement aux réunions de section de l'avancée de vos travaux.

Vos conclusions sont attendues pour le 15 décembre 2018, avec une note d'étape contenant vos premières idées de proposition d'ici le 15 juillet.

Luc ROUSSEAU

Copie : M. le président de la section Technologie et Société

Annexe 2 : Liste des acronymes utilisés

ACPR	Autorité de contrôle prudentiel et de résolution
AFAI	Association Française de l'Audit et du conseil Informatique
AMF	Autorité des marchés financiers
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	Application programming interface
BCR	Binding Corporate Rules
BDES	Base de données économiques et sociales
CEA	Commissariat à l'énergie atomique et aux énergies alternatives
CGE	Conseil général de l'économie
CGU	Conditions générales d'utilisation
CIGREF	Club informatique des grandes entreprises françaises
CJCE	Cour de justice des Communautés européennes
CJUE	Cour de justice de l'Union européenne
CMF	Code monétaire et financier
CNAM	Conservatoire national des arts et métiers
CNI	Conseil national de l'industrie
CNIL	Commission nationale de l'informatique et des libertés
CNRS	Centre national de la recherche scientifique
COFRAC	Comité français d'accréditation
CSP	Code de la santé publique
DAF	Direction administrative et financière
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
DGE	Direction générale des entreprises
DPO	Data Protection Officer, délégué à la protection des données
DSP	Directive sur les services de paiement
EIVP	Etude d'impact sur la vie privée
FBF	Fédération Bancaire Française
GAFA(M)	Google, Amazon, Facebook, Apple (,Microsoft)
INRIA	Institut national de recherche en informatique et en automatique
ISO	Organisation internationale de normalisation
LIL	Loi Informatique et Libertés
MOOC	Massive open online course
MR	Méthodologie de référence
NIR	Numéro d'inscription au Répertoire
OMS	Organisation mondiale de la santé
PIA	Privacy Impact Assessment
RGPD	Règlement général sur la protection des données
SaaS	Software as a Service
SI	Système d'information
Tracfin	Traitement du renseignement et action contre les circuits financiers clandestins

Annexe 3 : Liste des personnes rencontrées ou interrogées

Organismes publics et parapublics

ACPR (Jean-Philippe Barjon, Pierre Bienvenu et Caroline Bontems)
Alsace Biovalley (Guillaume Facchi, Marie-Charlotte Lechner)
CNIL (Sophie Nerbonne, Gwendal Le Grand)
Direction Générale des entreprises (Chantal Rubin)
Ministère de la Santé (Jean-Yves Fagon)
Ministère de l'Intérieur (Fabrice Mattatia)

Organisation professionnelles

Cap Digital (Françoise Colaïtis)
EIT Health (Jean-Marc Bourez)
FEVAD (François Momboisse)
Ordre des experts comptables (Christian Scholer, Sanaa Moussaïd et Gaelle Patetta)
SNITEM (Florent Surugue, David Ravanne et Manuela Olive)

Entreprises

Amazon (Mathieu Jeandron)
AXA (Fabrice Perrin)
Biotronik (Florelle Repiton)
Crédit Agricole (Marie Lhuissier, Marie-Françoise Chabriol, Dominique Moreau-Ferellec et Christian Coutand)
DTF Medical (Jean-Philippe Massardier)
Google France (Olivier Esper)
HDC (Henri Delahaie)
HSBC (Régis Vialelle)
Lydia (Alison Alonso)
MAIF (Stéphane Grégoire)
Roche (Sylvia Caccia et Mireille Violleau)
Sigvaris (Aurélie Budiscak)
Société Générale (Antoine Pichot)
Visible Patient (Luc Soler)
Voluntis (Nicolas Bertrand)
Yomoni (Sébastien D'Ornano)

Professionnels

Frédéric Barbot (Praticien Hospitalier)
Claire Levallois Barthe (Institut Mines Telecom)
Anne-Marie Benoit (UMR PACTE, CNRS)
Guillaume Buffet (ancien président de Renaissance numérique)
Thomas Dautieu (directeur adjoint conformité CNIL)

Sylvia Pelayo (Université du Droit et de la Santé Lille 2)
Michel Toussaint (Directeur des Systèmes d'Information de la Clinique de Strasbourg)

Associations

France FinTech (Alain Clot, Kristen Charvin)

Annexe 4 : Les droits fondamentaux issus du RGPD[97]

Le droit à l'information

L'article 12 du RGPD dispose que le responsable de traitement doit fournir à la personne concernée des informations « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant ». Les articles 13 et 14 détaillent les informations à fournir selon que les données sont collectées auprès de la personne concernée ou selon un autre moyen.

Le droit d'accès aux données

L'article 15 du RGPD dispose que toute personne peut demander à un responsable de traitement si des données la concernant sont traitées, et obtenir des informations sur le traitement ainsi qu'une copie des données la concernant et toute information disponible sur leur origine.

Il existe cependant certaines exceptions au droit d'accès : si le délai légal de conservation des données est expiré, si les droits et libertés d'une autre personne sont mis en danger, en cas de demande « objectivement abusive » (toutefois, aucune disposition ne prévoit de pouvoir prouver que l'exception n'est pas abusée).

Enfin, la vérification de l'identité des personnes concernées par le droit d'accès peut soulever des difficultés pratiques. Il n'existe pas de modèles de formulaires de demande d'accès et de réponse aux demandes. Le risque potentiel est que les entreprises n'informent les personnes concernées qu'à minima. Elles pourraient en outre prétendre que les demandes n'ont pas été bien formulées et collecter par là même des données sensibles en prétendant en avoir besoin pour d'éventuelles vérifications d'identité.

Le droit de rectification

L'article 16 du RGPD dispose que toute personne peut exiger que les données la concernant soient rectifiées, complétées ou mises à jour. Le responsable de traitement en informe chaque destinataire des données (sauf si cela se révèle impossible ou exige des efforts disproportionnés[98]).

Le droit d'effacement

Selon l'article 17 du RGPD, la personne concernée peut exiger que les données la concernant soient effacées dans les cas suivants :

- les données ne sont plus nécessaires à la finalité ou sont traitées d'une autre manière ;
- la personne concernée retire le consentement sur lequel était basé le traitement ;
- la personne s'oppose à un traitement de prospection, ou elle s'oppose à un traitement effectué pour une mission d'intérêt public ou d'autorité publique, ou dans l'intérêt légitime du responsable du traitement, sans qu'un motif légitime impérieux justifie de rejeter l'opposition ;
- le traitement est illicite ;

---

[97] Source : RGPD et droit des données personnelles, Fabrice Mattatia, Eyrolles, 2018

[98] Article 19 du RGPD

- les données doivent être effacées pour respecter une obligation légale ;
- les données ont été collectées par un service de la société de l'information et concernent un mineur.

Le droit d'opposition

La personne concernée peut s'opposer au traitement :

- si le traitement est basé sur le consentement, en retirant son consentement à tout moment[99] ;
- si le traitement est basé sur l'intérêt public ou sur les intérêts légitimes du responsable de traitement, le droit d'opposition s'applique[100] (ce droit est absolu en cas de prospection) ;
- dans le cas d'un contrat, en se référant aux clauses de renonciation du contrat ;
- en exerçant le droit à l'effacement qui est absolu dans certains cas précisés ci-dessus.

Le droit à la limitation du traitement

L'article 18 du RGPD introduit la notion de « limitation ». La limitation d'un traitement consiste à ne traiter les données qu'avec le consentement de la personne concernée, ou pour l'exercice d'un droit en justice, pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public. La personne concernée a le droit d'obtenir du responsable de traitement la limitation du traitement :

- dans le cas où elle conteste l'exactitude des données pendant le délai nécessaire à l'exercice du droit de rectification ;
- si le traitement est illicite et que la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;
- si le responsable du traitement n'a plus besoin des données aux fins du traitement mais qu'elles sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice.

Le droit à la portabilité des données à caractère personnel fournies

L'article 20 du RGPD prévoit que « les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement ». Ce droit n'existe que lorsque le traitement est automatisé et est basé sur le consentement ou sur un contrat.

[99] Article 7 du RGPD

[100] Article 21 du RGPD

Annexe 5 : Les « marges de manœuvre » autorisées par le RGPD

La présente annexe comporte la liste des renvois du RGPD aux législations nationales, suivie de l'indication des principales options retenues par la France.

Les 56 marges de manœuvre :

1) Pour les règles sectorielles spécifiques des États membres, notamment pour les données sensibles et les conditions de licéité, et la marge de manœuvre des États membres : considérant 10 ;

2) Pour la prise en compte des besoins spécifiques des TPE/PME : considérant 13 ;

3) Pour adapter le règlement pour le secteur public, y compris pour adopter des conditions spécifiques ou des restrictions : considérant 19 ; article 6, paragraphe 2 ;

4) Pour désigner certains responsables de traitement : article 4, point 7 ;

5) Pour les traitements de données par les juridictions et la supervision de ceux-ci : considérant 20 ;

6) Pour les données des personnes décédées : considérant 27 ;

7) Pour les tiers autorisés : considérant 31 et article 4, point 9 ;

8) Pour la licéité des traitements du secteur public (dans l'intérêt public ou imposant une obligation légale) et la création de tels traitements : considérants 45, 47 ; article 6, paragraphe 3 ;

9) Pour déterminer la compatibilité, la licéité et la base légale des traitements de données ultérieurs dans l'intérêt public : considérants 50, 51 ; article 6, paragraphe 4 ;

10) Pour les conditions relatives au consentement des enfants de moins de 16 ans et de plus de 13 ans : article 8, paragraphe 1er ;

11) Pour les traitements de données sensibles, y compris de santé, génétiques ou biométriques : considérants 51, 52, 53, article 9, articles 17 pour les limitations au droit à l'oubli et 21, paragraphe 6 pour les traitements de données sensibles à des fins scientifiques, statistiques ou historiques dans l'intérêt privé ;

12) Pour le traitement des données relatives aux condamnations pénales : article 10 ;

13) Pour déterminer les conséquences de demandes d'exercice de droits excessives ou manifestement infondées : article 12 ;

14) Pour l'obtention ou la divulgation d'information par le responsable de traitement : article 14, paragraphe 5, point c) ;

15) Pour la compilation des opinions politiques dans le cadre des activités électorales : considérant 56 ;

16) Pour le droit à l'effacement et le droit à l'oubli : considérant 65 et article 17 ;

17) Pour la limitation du traitement des données au lieu de l'effacement : article 18 ;

18) Pour autoriser le profilage : considérant 73 et article 22 ;

19) Pour les restrictions aux droits des personnes et obligations des responsables de traitement : considérant 59 et article 23 ;

20) Pour déterminer les responsabilités respectives des responsables de traitement conjoints : article 26 ;

21) Pour déterminer les exigences sur la validité juridique d'un acte liant le responsable de traitement au sous-traitant : considérant 81 et articles 28 et 29 ;

22) Pour les exigences relatives aux instructions du responsable de traitement à son sous-traitant, y compris pour obliger le sous-traitant à conserver les données après la fin du contrat avec le responsable de traitement : considérant 81 et article 28 ;

23) Pour la sécurité des traitements : article 32 ;

24) Pour prévoir des analyses d'impact dans le cadre de l'adoption d'une législation nationale : considérant 93 et article 35 ;

25) Pour la procédure de consultation préalable de l'autorité de contrôle dans le cadre de l'adoption d'une nouvelle législation ou de la mise en place d'un nouveau traitement de données dans l'intérêt public : article 36 ;

26) Pour obliger à la désignation d'un délégué à la protection des données : article 37 ;

27) Pour l'obligation de secret professionnel du délégué à la protection des données : article 38 ;

28) Pour encourager les codes de conduite et la certification : articles 40 et 42 ;

29) Pour l'accréditation des organismes certificateurs : article 43 ;

30) Pour conclure des accords internationaux : considérant 102 et article 46 ;

31) Pour des transferts de données dans l'intérêt public : considérant 111 ;

32) Pour certains transferts dérogatoires : article 49 ;

33) Pour limiter les transferts de données vers un pays tiers ou une organisation internationale en l'absence de décision d'adéquation à certaines catégories : considérant 112 ; article 49 ;

34) Pour la création des autorités de contrôle : considérant 117 ;

35) Pour prévoir la coopération entre les autorités de protection des données nationales s'il en existe plus d'une : considérant 119, article 51 ;

36) Pour les conditions générales de désignation des membres et du personnel des autorités de contrôle : considérant 121, articles 51, 52, 53, 54 ;

37) Pour les pouvoirs des autorités de contrôle : considérant 129, article 58 ;

38) Pour les instances auxquelles les autorités de contrôle font rapport : article 59 ;

39) Pour confier des pouvoirs d'enquête aux autorités de contrôle des autres États membres effectuant des enquêtes sur son territoire dans le cadre d'opérations conjointes : article 62 ;

40) Pour la désignation de l'autorité de protection des données participant au CEPD lorsqu'il y en a plusieurs : considérant 119 et article 68 ;

41) Pour les actions collectives et pour les exigences concernant les associations pouvant agir en représentation : considérant 142, article 80 ;

42) Pour la désignation de la juridiction compétente sur le territoire : considérant 143 ; articles 78 et 82 ;

43) Pour les régimes de responsabilité : considérant 146, article 82 ;

44) Pour les sanctions administratives des responsables de traitement publics : considérants 150 et article 83 paragraphe 7 ;

45) Pour prévoir des sanctions lorsque le Règlement n'a pas harmonisé les sanctions, y compris pénales : considérants 149 et 151 et article 84 ;

46) Pour l'articulation des dérogations nationales en matière de liberté d'expression et de droit à l'information et les dérogations spécifiques : considérant 153 ; article 85 ;

47) Pour l'accès aux documents publics et la réutilisation des données du secteur public : considérant 154 et article 86 ;

48) Pour fixer les conditions spécifiques du traitement d'un numéro national d'identification : article 87 ;

49) Pour les traitements de données des salariés : considérant 155 ; article 88 ;

50) Pour les traitements des données à des fins archivistiques dans l'intérêt public, statistiques, scientifiques, historiques, pour prévoir les garanties appropriées nécessaires et les dérogations : considérant 156, article 89 (et articles 14 et 17) ;

51) Pour la recherche scientifique : considérant 157 ;

52) Pour les traitements de données à des fins archivistiques dans l'intérêt public : considérant 158 ;

53) Pour les traitements de données à des fins statistiques : considérant 162 ;

54) Pour les statistiques publiques : considérant 163 ;

55) Pour limiter les pouvoirs des autorités de contrôle pour respecter le secret professionnel : considérant 164 et articles 13, paragraphe 5, point d) et 90 ;

56) Pour les traitements de données des églises et associations religieuses : considérant 165.

Les principales options retenues par la France[101] :

L'encadrement des décisions prises par un algorithme

L'article 22 du RGPD qui donne le droit aux personnes de ne pas faire l'objet d'une décision uniquement prise par un algorithme prévoit une exception en laissant une marge de manœuvre aux Etats membres. La France s'est saisie de cette occasion pour ouvrir la participation d'algorithmes aux prises de décisions en matière de décisions administratives[102].

[101] cf. La Semaine Juridique Administrations et Collectivités territoriales n° 27, 9 Juillet 2018, 2199

[102] Reformulation de l'article 10 de la loi du 6 janvier 1978

L'action de groupe en matière de données personnelles devient une réalité en droit français

Auparavant, lorsqu'un responsable de traitement ne respectait pas les obligations de la loi Informatique et Libertés, chaque personne concernée devait lancer une procédure individuellement. De telles démarches n'étaient clairement pas incitatives. Avec le RGPD[103], il est possible d'entreprendre des actions collectives afin d'exiger la cessation d'un manquement, menées par des organisations mandatées par les personnes concernées. Chaque Etat dispose d'une marge de manœuvre et détermine si des organisations peuvent mener des actions sans être mandatées et si les actions collectives peuvent avoir pour but la réparation d'un préjudice.

Précédemment cantonnée à la cessation du manquement commis par le responsable du traitement ou le sous-traitant, l'action de groupe permet désormais d'obtenir la réparation des préjudices matériels et moraux subis par les personnes concernées[104] (mais la responsabilité de la personne ayant causé le dommage ne pourra être engagée que si le fait générateur du dommage est postérieur au 25 mai 2018).

Le consentement des mineurs

Le RGPD laisse aux Etats membres la possibilité d'abaisser l'âge minimal à partir duquel un mineur peut consentir à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information[105] (pas en-dessous de 13 ans). En France, la majorité numérique est fixée à 15 ans[106]. Pour les mineurs âgés de moins de 15 ans, la nouvelle loi exige que le consentement soit donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur.

Les données à caractère personnel relatives aux condamnations pénales et aux infractions

L'article 10 du RGPD soumet à un régime d'autorisation le traitement des données personnelles relatives aux condamnations pénales et infractions. Tout en reproduisant la définition du règlement européen, la loi du 20 juin 2018 élargit la liste des institutions et personnes autorisées à traiter des données pénales[107].

Le consentement des utilisateurs de smartphones

L'article 28 de la loi du 20 juin 2018 est une application directe de l'article 7 du RGPD. Il contraint les fabricants et distributeurs de smartphones à proposer davantage de choix dans les applications à destination des consommateurs et vise en particulier les éditeurs d'applications préinstallées sur les terminaux.

Le traitement du numéro de sécurité sociale (NIR)

Comme l'article 87 du RGPD le permet, la loi française prévoit des formalités particulières concernant le numéro de sécurité sociale. La loi du 20 juin 2018 (nouvel article 22) dispose qu'un décret en Conseil d'État, pris après avis motivé et publié de la CNIL, détermine les catégories de responsables de traitement et les finalités de ces traitements au vu desquelles ces derniers peuvent être mis en

[103] Article 80 du RGPD

[104] L'article 25 de la Loi du 20 juin 2018 renforce l'article 43 ter de la Loi du 6 janvier 1978 relatif à l'action de groupe

[105] Article 8 du RGPD

[106] Article 7-1 de la loi n°78-17 du 6 janvier 1978

[107] Loi 78-17 article 9, al. 1 modifié

œuvre lorsqu'ils portent sur des données comportant le NIR. Cependant, les traitements à finalité exclusive de statistique publique, les traitements de recherche scientifique ou historique et les démarches administratives en ligne ne sont pas concernés et dépendent directement du RGPD (avec inscription au registre et analyse d'impact).

La liberté d'expression

L'article 85 du RGPD dispose que les Etats membres concilient le droit à la protection des données personnelles et le droit à la liberté d'expression et d'information. La loi Informatique et Libertés prévoit ainsi des dérogations pour les traitements de données personnelles concernés.

Biométrie et génétique

Le RGPD inclut les données biométriques et génétiques parmi les données sensibles. La loi dispose désormais (article 27) que les traitements mis en œuvre par l'État dans l'exercice de ses prérogatives de puissance publique et portant sur des données génétiques ou des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes, sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la CNIL.

Les collectivités territoriales

Le RGPD permet de désigner un même DPO pour plusieurs collectivités. L'article 31 de la loi du 20 juin 2018 autorise les collectivités territoriales et leurs groupements à conclure des conventions ayant pour objet la réalisation de prestations de service liées au traitement de données à caractère personnel, et à se doter d'un service unifié ayant pour objet d'assumer en commun les charges et obligations liées au traitement de données à caractère personnel[108].

[108] Sans préjudice du dernier alinéa de l'article L. 5111-1 du CGCT

Annexe 6 : Durées de conservation des données à caractère personnel

Le présent document de travail[109], émanant d'une entreprise privée, a pour objet de référencer les différentes durées de conservation des données à caractère personnel traitées. Ces durées de conservation peuvent être déterminées par la loi (code du travail, code monétaire et financier…) ou ont été inspirées par la CNIL. La mission n'a pas identifié de version officielle et à jour d'un tel document, pourtant essentiel à la mise en conformité d'une entreprise avec le RGPD.

Finalité du traitement	Durée de conservation	Fondement juridique
Communication externe		
Données nécessaires à la gestion d'un site internet (identité des visiteurs, données de connexion…)	1 an	DI-007 Article 3 du décret n° 2011-219 du 25 février 2011
Gestion d'un fichier client	Les données des clients sont conservées au maximum pendant le temps de la relation commerciale. Elles peuvent être conservées à des fins de prospection commerciale au maximum pendant **3 ans** à compter de la fin de cette relation commerciale (par exemple, à compter d'un achat, de la date d'expiration d'une garantie, du terme d'un contrat de prestations de services ou du dernier contact émanant du client).	NS-048
Constitution et gestion d'un fichier de prospects non client (ex : envoi de sollicitations tels que l'emailings, appels téléphoniques, télécopies, SMS, etc.)	Au maximum **3 ans** à compter de leur collecte par le responsable de traitement ou à compter du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel) Attention : l'ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect	NS-048

[109] Source : https://www.argedis.com/wp-content/uploads/2018/06/WS.007-Dure%CC%81e-de-conservation-donne%CC%81es.pdf

Statistiques de mesures d'audience Les informations stockées dans le terminal des utilisateurs (ex : cookies) ou tout autre élément utilisé pour identifier les utilisateurs et permettant de les tracer	13 mois au maximum	NS-048
Gestion d'une lettre d'information	Jusqu'à désabonnement de la personne concernée (maximum)	Article 6-5° de la loi n°78-17 modifiée
Gestion d'une liste d'opposition au démarchage téléphonique	3 ans à compter de l'inscription dans la liste (maximum)	NS-048
Contrats conclus entre commerçants ou entre commerçants et non-commerçants (Tous les documents contractuels, contrats et conventions conclus dans le cadre d'une relation ou correspondance commerciale) **Fichiers de Fournisseurs** (identité du fournisseur, sa vie professionnelle, les éléments de facturation et de règlement)	5 ans (durée précise)	Article L110-4 du Code de commerce NS-048 DI-004
Réclamations et demandes de droit (accès, rectification, opposition et autres droits du chapitre III du RGPD) des personnes concernées par un traitement	Durée strictement nécessaire	

Gestion du personnel		
Registre unique du personnel	5 ans à partir du départ du salarié (durée précise)	Article R.1221-26 du code du travail
Gestion administrative des personnels (dossier professionnel, annuaires, élections professionnelles…)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Mise à disposition d'outils informatiques (suivi et maintenance des matériels, annuaires informatiques, messagerie électronique, intranet…)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Organisation du travail (agendas professionnels, gestion des tâches)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Gestion des carrières (date et conditions d'embauche ou de recrutement, date, objet et motif des modifications apportées à la situation professionnelle de l'employé, simulation de carrière, desiderata de l'employé en termes d'emploi…)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Formation des personnels (diplômes, certificats et attestations, langues étrangères pratiquées, suivi des demandes de formation professionnelle et des périodes de formation effectuées, organisation des sessions de formation, évaluation des connaissances et des formations)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Evaluation professionnelle de l'employé (dates des entretiens d'évaluation, identité de l'évaluateur, compétences professionnelles de l'employé, objectifs assignés, résultats obtenus, appréciation des aptitudes professionnelles sur la base de critères objectifs et présentant un lien direct et nécessaire avec l'emploi occupé, observations et souhaits formulés par l'employé, prévisions d'évolution de carrière)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Suivi administratif des visites médicales des employés	Temps de la période d'emploi de la personne concernée (maximum)	NS-046

Organisation du travail du personnel (annuaires internes et organigrammes, agendas professionnel, tâches des personnels, gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Registre unique du personnel	5 ans à partir du départ du salarié (durée précise)	Article R.1221-26 du code du travail
Gestion de l'annuaire du personnel	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Constitution d'une cellule de crise	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Sanctions disciplinaires	3 ans (durée précise)	Article L 1332-5 du Code du travail
Observations ou mises en demeure de l'inspection du travail	5 ans (durée précise)	Article D.4711-3 du code du travail
Casier Judiciaire (B3)	En l'absence d'un texte spécifique prévoyant la vérification des casiers judiciaires des employés : production du casier lors de l'entretien mais pas de conservation (La mention des vérifications des casiers effectuées dans le fichier de gestion du personnel sous la forme "oui/non" est suffisante)	CNIL (site internet)
Gestion des œuvres sociales et culturelles	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Activité des comités d'entreprise (données des employés : identification situation familiale, éléments professionnels et financiers)	Période d'admission du salarié au bénéfice des prestations sociales et culturelles (maximum) Période glissante de deux ans maximum à compter de l'exécution de la prestation pour l'historique de l'utilisation de ces prestations et le suivi des commandes par les salariés.	DI-010

Elections professionnelles	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Gestion des réunions des instances représentatives du personnel	Les données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation ne sont pas conservées au-delà de la période de sujétion de l'employé concerné	NS-046
Mandats des représentants du personnel (nature du mandat et syndicat d'appartenance)	6 mois après fin du mandat (durée précise)	Article L 425-1 du Code du travail Article L 2411-5 du Code du travail
Fichiers de recrutement (procédure de recrutement ayant aboutie ou non)	2 ans après le dernier contact avec le candidat (maximum)	Recommandation n° 02-017 du 21 mars 200 2
Procédure de signalement interne (lanceur d'alerte)	Lorsqu'une alerte est considérée comme n'entrant pas dans le champ du dispositif dès son recueil par le responsable de traitement, les données la concernant doivent immédiatement être supprimées ou archivées après anonymisation. Lorsqu'une alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, la suppression ou l'archivage après anonymisation doit intervenir dans un délai de deux mois après la clôture des vérifications, dans les conditions détaillées par la délibération.	AU-004

Badges sur le lieu de travail et contrôle d'accès sur les lieux de travail		
Contrôle des horaires (éléments d'identification)	5 ans après le départ du salarié (maximum)	NS-042
Contrôle des horaires (données utilisées pour le suivi du temps de travail, y compris les données relatives aux motifs des absences)	5 ans (maximum)	NS-042
Contrôle d'accès (Eléments relatifs aux déplacements des personnes)	3 mois (maximum)	NS-042
Données relatives au paiement des repas	3 mois pour les données monétiques et 5 ans en cas de paiement par retenue sur salaire (maximum)	NS-042
Contrôle d'accès sur les lieux de travail avec maîtrise de la personne sur son gabarit biométrique (Contrôle d'accès par empreinte digitale aux ordinateurs portables professionnels, réseau veineux de la main sur les lieux de travail, empreinte digitale sur le lieu de travail, contrôle d'accès par contour de la main aux lieux de travail)	Le gabarit biométrique ne peut être conservé que le temps de l'habilitation de la personne concernée et doit être supprimé à son départ. Les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservées cinq ans après le départ de la personne disposant d'une habilitation d'accès de longue durée, et 3 mois après le départ des personnes disposant d'une habilitation d'accès ponctuelle. Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de 3 mois.	AU-052
Contrôle d'accès sur les lieux de travail, avec conservation des gabarits biométrique en base	Le gabarit biométrique ne peut être conservé que le temps de l'habilitation de la personne concernée et doit être supprimé à son départ. Les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservées cinq ans après le départ de la personne disposant d'une habilitation d'accès de longue durée, et 3 mois après le départ des personnes disposant d'une habilitation d'accès ponctuelle. Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de 3 mois.	AU-053

Gestion des outils informatiques et de la téléphonie		
Annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Données de connexion enregistrées pour assurer la sécurité et le bon fonctionnement des applications et des réseaux informatiques (à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Contrôle de l'utilisation d'internet par les salariés (historique des connexions et les logs de connexion des salariés)	6 mois (maximum)	CNIL https://www.cnil.fr/fr/le-controle-de-lutilisation-dinternet-et-de-la-messagerie-electronique
Gestion de l'intranet	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Gestion de la messagerie électronique (carnet d'adresses, comptes individuels, à l'exclusion de toute donnée relative au contrôle individuel des communications électroniques émises ou reçues par les employés)	Temps de la période d'emploi de la personne concernée (maximum)	NS-046
Contrôle de l'utilisation de la messagerie	6 mois (maximum)	Guide de la CNIL pour les employeurs et les salariés 2010
Gestion de la téléphonie (données relatives à l'utilisation des services de téléphonie : numéros appelés, numéros des appels entrants, identité de l'utilisateur du service téléphonique…)	1 an courant à la date de l'exigibilité des sommes dues en paiement des prestations des services de téléphonie (durée précise)	NS-047 et Article L. 34-2 du code des postes et des communications électroniques

Autocommutateur (détail des appels téléphoniques)	6 mois glissant	NS-047
Géolocalisation des véhicules professionnels (historique des déplacements)	Conservation des données en principe pendant deux mois maximum après la fin de la prestation **mais** durée de conservation : d'1 an maximum de l'historique des déplacements en vue de l'optimisation des données ; d'1 an ou plus dans le cadre d'une réglementation spécifique ou si une telle conservation est nécessaire pour prouver l'exécution d'une prestation lorsqu'il n'existe aucun autre moyen ; de 5 ans dans le cadre du suivi du temps de travail, seuls les horaires sont conservés.	NS-051

Sécurité des biens et des personnes		
Vidéosurveillance	1 mois (maximum)	Loi 95-73 du 21-01-1995

Gestion du paiement		
Conservation des numéros de carte bancaire par les commerçants	Suppression une fois la transaction réalisée (suppression dès le paiement effectif) MAIS le numéro de la carte et la date de validité peuvent être conservés pour une finalité de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires, pour une durée de 13 mois suivant la date de débit ou 15 mois en cas de paiement à débit différé.	Délibération n° 2017-222 du 20 juillet 2017 Article L 133-24 du Code monétaire et financier
Cryptogramme visuel	Conservation interdite, dans tous les cas de figure, y compris pour les abonnements nécessitant différents paiements.	Délibération n° 2017-222 du 20 juillet 2017

Archivage		
Données conservées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques	Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le RGPD (pseudonymisation, minimisation de la collecte, gestion des habilitations…) Lorsque ces finalités peuvent être atteintes en anonymisant les données, l'anonymisation doit être préférée.	Articles 5 e) et 89 du RGPD

Anonymisation		
Données anonymisées de manière irréversible	Indéfiniment	Avis 05/2014 du G29 sur les Techniques d'anonymisation adopté le 10 avril 2014

Annexe 7 : La gestion des documents papiers

Le RGPD s'applique aux données à caractère personnel, qu'elles soient numériques ou physiques (les documents papiers sont donc concernés), tout au long du processus de traitement (collecte, enregistrement, conservation, consultation, mise à jour, échange). Les risques de sécurité concernant les documents papiers sont bien réels. Selon un rapport de 2014 réalisé par *PwC* en collaboration avec *Iron Mountain*[110] fondé sur une enquête réalisée auprès des entreprises moyennes européennes concernant la perception et la gestion des risques de l'information, les 2/3 des personnes interrogées déclarent que la gestion des risques liés aux documents papiers est une préoccupation prioritaire. Entre juillet et septembre 2016, 40% des incidents liés à la sécurité des données au Royaume-Uni concernent des documents papiers[111] (erreur de destinataire, conservation des données dans un lieu non sécurisé, perte et vol de documents, suppression non sécurisée de documents…).

Les principaux freins à la bonne gestion des documents papiers

La gestion des documents papiers implique quelques difficultés :

- Un tri des données est nécessaire afin de respecter la finalité du traitement et ainsi empêcher d'éventuelles utilisations pour d'autres finalités non consenties. Or, un document papier peut contenir plusieurs types de données, ce qui complique le tri.
- L'impression de documents papiers rend les données accessibles physiquement, ce qui peut poser un souci de sécurité (vol, copie…). Se pose également le problème de l'accès aux données (qui sont censées être en théorie restituables facilement en cas de demande) et de leur classement lorsque leur nombre est très important.
- La suppression des documents papier peut constituer un obstacle car les démarches de suppressions conformes peuvent être longues, laborieuses, inefficaces ou pas assez sécurisées. Il conviendrait de mettre en place un dispositif sécurisé d'élimination des documents (avec stockage et transport sécurisés, destruction aux normes, certificat de destruction et traçabilité des opérations). La suppression des documents (pour des raisons d'obsolescence ou de confidentialité) doit être tracée et certifiée pour prévenir toute faille de sécurité[112].
- La sécurisation des données papiers est difficile à assurer (lieu adapté, sécurisé).
- L'importance des documents papiers peut être sous-estimée, car ceux-ci sont quelque peu banalisés dans divers usages courants. Il y a un manque de sensibilisation sur les risques et les instructions à suivre pour la suppression des documents papiers (bonnes pratiques, procédures de sécurité, etc.).

---

[110] https://fr.slideshare.net/mobile/lesechos2/7-au-dela-des-bonnes-intentionsrapport-completfr36p-def

[111] Sur 598 incidents relatifs à la protection des données enregistrés entre juillet et septembre 2016 par *l'Information Commissioner's Office*

[112] Norme DIN 66399 : https://www.terface.com/media/fiches_technique/fiche-norme-66399.pdf

Pour pallier ces problèmes, le RGPD ouvre la voie de la digitalisation

La numérisation des documents papiers est une alternative envisageable, notamment pour faciliter la localisation des données (avec les systèmes automatisés de recherche). La « numérisation fidèle » permet de détruire les documents originaux papiers sous réserve de constituer des copies fiables qui seront conservées dans des conditions adaptées pour préserver leur intégrité[113]. Toutefois, la digitalisation est un réel investissement, car elle est coûteuse tant en temps qu'en argent, et correspond à un changement radical des habitudes (l'utilisation du papier étant très majoritaire).

Si le passage à la numérisation peut paraître complexe[114], il est un moyen efficace de se conformer au RGPD. Il peut en outre s'agir d'une opportunité pour créer de nouvelles activités autour de la transformation numérique des documents papiers (aujourd'hui relativement falsifiables) visant à améliorer leur sécurité et leur conformité (pour des raisons de preuve, de comptabilité ou d'obligations fiscales).

[113] https://fr.wikipedia.org/wiki/NF_Z_42-013 ; https://locarchives.fr/actualites/lafnor-annonce-la-publication-de-la-norme-nf-z42-026/

[114] https://www.openbee.com/media/Ebook_Guide_des_bonnes_pratiques_OpenBee.pdf

Annexe 8 : Le registre de traitement des données à caractère personnel

Le registre de traitement des données est un document qui formalise la façon dont les données personnelles sont exploitées au sein d'une organisation. « L'article 30 du RGPD instaure l'obligation pour le responsable de traitement de tenir un registre décrivant tous les traitements de données personnelles. Toutefois, les PME et TPE bénéficient d'une dérogation décrite au 5) de l'article 30 : ce point précise que l'obligation de registre ne s'applique pas à « *une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données exposées dans l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10* ». Il suffit qu'une de ces conditions soit remplie pour rendre obligatoire la tenue du registre… il est donc très facile d'avoir à tenir un registre (un simple système de prise de rendez-vous pour un coiffeur par exemple). Comme l'indique le G29, dans ce cas, le registre peut se limiter aux traitements ne bénéficiant pas de la dérogation[115].

Pour les PME/TPE concernées par la constitution d'un registre de traitements des données, il convient de rappeler qu'il doit comporter en priorité (un modèle de registre de traitement des données est disponible sur le site de la CNIL) :

- Les activités de l'entreprise qui nécessitent une exploitation des données personnelles.
- Les objectifs poursuivis lors de cette exploitation.
- Les types de données utilisées.
- Les personnes ayant accès à ces données.
- La durée de conservation des données.

[115] RGPD et droit des données personnelles, Fabrice Mattatia, 2018, Eyrolles