Focus sur les tenants et aboutissants du RGPD

Tout ce que vous devez savoir sur le RGPD (première partie).

Par Paul Salaun.

Ce que l'on appelle aujourd'hui le Règlement Général sur la Protection des Données (RGPD) est un Règlement de l'Union européenne du Parlement européen et du Conseil adopté le 27 avril 2016.

Ce règlement est relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation desdites données[1]. Le RGPD est ainsi censé constituer désormais le texte de référence en matière de protection des données à caractère personnel pour toute l'Union européenne. À partir du 25 mai 2018, date de son entrée en vigueur, le RGPD renforcera et unifiera le régime juridique de protection des données personnelles pour tous les ressortissants des états membres.

Cet article pourrait vous interesser

RGPD : le jeu trouble de Google met le géant américain sous le feu des critiques

Les objectifs principaux du RGPD sont simples. Il s'agit d'une part d'assurer une meilleure protection de la vie privée des internautes quant à la confidentialité de la masse de données personnelles les concernant. L'émission de ces données connait une forte croissance, notamment par le passage de Big-Data au Fast-Data. D'autre part il s'agit de rendre obligatoire cette protection par une responsabilisation des acteurs du traitement des données personnelles, s'il le faut par le prononcé d'amendes…

Afin de bien comprendre, de manière synthétique les objectifs mais également les freins à l'application du RGPD il convient d'en connaitre les origines et les principes. La confrontation de ces origines et de ces principes permet d'appréhender quelles sont les chances de réussites mais aussi les risques d'échecs de la mise en œuvre du RGPD.

Aux origines du RGPD, un souci de protection d'une confidentialité effective des données personnelles à l'origine du Big-Data

C'est assez tardivement au mois de janvier 2012 que la Commission européenne a pleinement pris conscience des enjeux de la protection de la confidentialité des données personnelles au regard du développement du Big-Data et déjà des prémices de son évolution irrémédiable vers le Fast Data. Fut ainsi constatée l'obsolescence de la Directive du 24 octobre 1995 sur la protection des données à caractère personnel[2].

La Commission a alors proposé au Parlement et au Conseil une réforme globale de la règlementation en matière de protection des données à caractère personnel. Cette évolution juridique s'articule autour de deux volets principaux. Le premier est celui de la modernisation des principes de protection des données à caractère personnel aujourd'hui archaïques et formulés en 1995, à l'époque des débuts de la vulgarisation de l'accès à Internet. Le second volet est celui de la création d'un nouveau Règlement destiné à assurer une protection effective des données à caractère personnel tout en permettant le bon déroulement des activités policières et judiciaires.

L'objectif général de ce nouveau texte est ainsi de redonner aux citoyens de l'Union européenne un contrôle effectif de leurs données à caractère personnel, tout en préservant et simplifiant l'environnement règlementaire des structures privées ou publiques traitant lesdites données.

Dans le cadre de cette démarche le Parlement adopte le 12 mars 2014 en première lecture une résolution législative sur

la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[3].

Il s'agit ici de la première étape de l'élaboration du RGPD. Cette résolution de mars 2014 est venue générer des négociations entre la Commission européenne, le Parlement et le Conseil. Ces discussions se sont étendues jusqu'au 15 décembre 2015. Cette démarche aboutira sur le Règlement du Parlement européen et du Conseil du 27 avril 2016

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[4].

C'est ce Règlement publié le 4 mai 2016 au JOUE qui prévoit l'entrée en vigueur du RGPD au 25 mai 2018.

Au cœur des enjeux de mise en œuvre du RGPD se trouve le développement du Big-Data, rejoint aujourd'hui par le Fast-Data. On appelle Fast-Data l'application des logiques d'analyses du Big-Data à de plus petits ensembles de données nécessitant d'être traités et analysés en temps réel dès qu'ils sont générés. Le Fast-Data a ainsi instauré une analyse en temps réel des données à caractère personnel, rendue

obligatoire par la multiplication notamment de l'usage des objets connectés et robots. Ces technologies collectent des données à caractère personnel de plus en plus rapidement et massivement. Il est dès lors capital pour les responsables du traitement des structures privées ou publiques de distinguer les données intéressantes à être stockées et conservées de celles qui doivent être analysées immédiatement pour se révéler utiles. Le Fast-Data est la technologie répondant à cette seconde possibilité d'exploitation des données à caractère personnel à l'instant où elles sont générées et donc avant qu'elles ne perdent leur intérêt.

La relation du RGPD au Big-Data et au Fast-Data présente deux enjeux majeurs. Le premier est celui de la mise en conformité des Data-Lakes au nouveau Règlement européen et le second est celui de l'anonymisation d'un maximum de données pour les faires sortir des obligations du RGPD.

Le RGPD prévoit ainsi, au sein des structures privées ou publiques, la nomination d'un délégué à la protection des données à caractère personnel, appelé le DPO. Dès avant le 25 mai 2018 ces délégués ont reçu la charge d'instaurer au plus vite des procédures destinées à répondre au potentiel grand nombre de demandes d'accès, de portabilité ou d'effacement de données à caractère personnel, ainsi qu'à la limitation de leur traitement. Feront particulièrement l'objet desdites procédures les Data-Lakes, lesquels du fait de leurs tailles stockent des milliers de données non forcement identifiées. Le RGPD vient imposer un recensement de l'ensemble de ces données, afin de déterminer s'il s'applique à celles-ci ou non.

Avec l'entrée en vigueur du RGPD le responsable du traitement des données à caractère personnel contenues dans les Data-Lakes devront répertorier l'emplacement exact où celles-ci sont stockées. Il faudra chercher à savoir si les personnes physiques ou morales objets de ces données sont identifiables ou non. Ainsi le RGPD viendra inévitablement développer le marché des logiciels de Data-Discovery, lesquels permettent d'identifier et de localiser tous les exports de base de données réalisés par et pour le compte d'organismes privés ou publics.

L'entrée en vigueur du RGPD va par ailleurs inévitablement accentuer le mouvement d'anonymisation des données personnelles. Dès lors que les entreprises, les administrations et les administrations disposeront d'une cartographie de leur Data-Lakes, celles-ci devront répondre au risque de piratages, de fuites et de disparitions non souhaitées desdites données personnelles.

L'une des méthodes pour limiter ce risque est l'anonymat des données personnelles. L'article 26 du RGPD énonce en ce sens que :

les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations

supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable.

L'application du RGPD va donc là aussi générer une augmentation de l'utilisation des logiciels d'anonymisation destinés à pallier à ces inconvénients.

Les différentes obligations générées par le RGPD

1. *Le champ d'application territoriale :*

   Le RGPD s'applique à l'ensemble des traitements de données à caractère personnel pratiqués par un responsable du traitement domicilié sur le territoire de l'Union européenne mais aussi du ou des sous-traitants à qui il a pu confier cette tâche. Peu importe par la suite que ce traitement ait effectivement lieu ou non sur le territoire de l'Union. En outre le RGPD est d'applicabilité générale sur le territoire de l'Union européenne dans les deux cas suivants. Le premier cas est celui des traitements de données personnelles concernant l'offre de biens ou de services à des personnes au sein de l'Union européenne, qu'un paiement soit exigé ou non en contrepartie de ces transactions. Le second cas très généraliste est celui du suivi du comportement des personnes physiques et morales, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. Le RGPD est ainsi devenu un puissant instrument de protection des libertés fondamentales dans le contexte du risque d'une inquisition numérique.

2. *Un RGPD susceptible d'une extraterritorialité :*

   Le RGPD vient premièrement instaurer un cadre harmonisé de la protection des données à caractère personnel. Il génère à ce sujet un seul bloc de règles juridiques, directement applicables à la protection desdites données. Ces textes étant issus d'un Règlement, ils n'ont pas besoin d'être transposés par les États membres de l'Union Européenne. Leur applicabilité est directe. Le RGPD supprime ainsi les différences de lois nationales concernant la protection des données à caractère personnel, lesquelles rendaient jusque-là impossible l'émergence d'un système unique de réglementation juridique.

   En lien avec ce premier principe de l'unification de règles juridiques concernant la confidentialité des données à caractère personnel, vient s'appliquer le principe d'extraterritorialité.

Désormais, à chaque fois qu'une personne physique ou morale établie au sein de l'Union Européenne fera l'objet d'un traitement de ses données à caractère personnel par un organisme public ou privé situé hors Union, le RGPD s'appliquera néanmoins. Cette solution était pressentie depuis que la CJUE dans son arrêt du 13 mai 2014 *« Google Spain et Google »* est partie du principe que les dispositions juridiques européennes en matière de traitement des données à caractère personnel s'appliquent aux responsables des traitements domiciliés hors union, même si ceux-ci estiment que n'étant pas établis au sein de l'Union, il ne devraient pas être astreints au respect de ses réglementations[5]. Pour que cette extraterritorialité soit possible il faut néanmoins que le droit d'un État membre de l'Union européenne s'applique en vertu du droit international public dans le pays où le responsable du traitement des données impactées est domicilié.

3. *Les traitements de données à caractère personnel concernés par l'application du RGPD :*

Sont concernés par l'application du RGPD d'une part les traitements de données à caractère personnel automatisés en tout ou en partie, ainsi que, d'autre part, les traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Le RGPD prévoit dans cette logique qu'il ne s'applique pas au traitement des données à caractère personnel dans quatre cas précis. Le premier cas est celui d'une activité ne relevant pas du champ d'application du droit de l'Union européenne. Ensuite, le RGPD ne s'applique pas aux États membres dans le cadre d'activités relèvant du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne concernant les dispositions relatives à la Politique Etrangère et de Sécurité Commune. Troisièmement le RGPD ne concerne pas également le traitement de données à caractère personnel par des personnes physiques dans le cadre d'une activité strictement personnelle ou domestique. Enfin, les obligations du RGPD ne s'appliquent pas aux autorités compétentes agissant à des fins de prévention, de détection ou de poursuite d'infractions pénales. Sont ici concernées également les autorités luttant pour la préservation de la sécurité publique.

En revanche, le RGPD s'applique à l'ensemble des traitements des données à

caractère personnel par les institutions, organes et organismes de l'Union, exception faites des dispositions du chapitre 2 du titre V TUE.

4. *Les critères de l'établissement et du ciblage :*

Les conditions d'applications du RGPD ont trait d'une part à l'établissement du responsable du traitement et de ses sous-traitants éventuels, ainsi d'autre part au ciblage pratiqué par ces traitements.

Sont concernés par le critère de l'établissement tous les responsables du traitement des données à caractère personnel (ainsi que leurs sous-traitants) établis sur le territoire de l'Union européenne.

Les traitements de données personnelles concernés par l'application du RGPD relèvent de la pratique du ciblage. Sont ainsi concernés tous les traitements ou sous traitements visant à fournir au sein de l'Union européenne des biens et services à des personnes physiques ou morales (et ce même à titre gratuit), ou à suivre leurs comportements à des fins publicitaires ou non.

5. *Le droit à la communication des données personnelles :*

Le RGPD affirme un droit d'accès pour toute personne physique ou morale concernée par le stockage et/ou le traitement de données personnelles. C'est alors à cette même personne de solliciter le responsable du traitement si elle désire que lesdites données lui soient communiquées. Cette personne peut également à cette fin mandater une tierce personne de son choix pour exercer son droit d'accès.

Lorsqu'une demande de communication est effectuée via un mandat, l'auteur de celle-ci doit présenter un écrit décrivant l'objet du mandat relatif à l'exercice du droit d'accès. Sont alors mentionnées les identités du demandeur exerçant son droit d'accès ainsi que celle du mandataire. Lorsque lesdites données concernent des mineurs et des majeurs sous tutelle, ce sont les parents ou le tuteur qui effectuent cette démarche.

Avec l'entrée en vigueur du RGPD en son article 12.3, les responsables du traitement des données ne bénéficieront plus que d'un mois maximum pour répondre à une telle demande. Ce délai commencera à courir à compter de la réception de la demande de communication. Le même article du RGPD énonce que ce délai pourra être prolongé en fonction de la complexité et du nombre de demandes effectuées. La condition posée pour prolonger ce délai sera d'informer la personne concernée dans le mois qui suit sa demande de droit d'accès.

Obéit enfin à un régime spécifique le traitement des données concernant les dossiers médicaux. Ici les délais sont différents. En application de l'article L 1111-7 du Code de la santé publique, la communication du dossier médical doit être effectuée au plus tard dans les 8 jours suivant la demande et au plus tôt dans les 48 heures. Lorsque les données remontent à plus de cinq années, le délai de transmission est porté à deux mois.

6. *La portabilité des données personnelles :*

Le RGPD est venu introduire au sein de l'Union européenne un droit à la portabilité des données à caractère personnel. Ce droit reconnu à chaque citoyen de l'Union européenne est défini à l'article 20 du RGPD. Il offre premièrement la possibilité de recevoir du responsable du traitement les données nous concernant pour les utiliser à notre bénéfice propre. Ce droit permet d'autre part le transfert direct des données personnelles d'un responsable de traitement à un autre responsable de traitement ou à un environnement IT sans obstacle lorsque la réclamation en est faite.

Les données concernées sont les suivantes. D'une part sont concernées par le RGPD les données que la CNIL présente comme

> *déclarées activement et consciemment par la personne concernée, telles que des données fournies pour créer un compte en ligne*[6].

La CNIL précise en outre que sont aussi concernées

> *les données générées par l'activité de la personne concernée, lorsqu'elle utilise un service ou un appareil (par exemple les données brutes collectées par des compteurs communicants, les achats enregistrés sur*

une carte de fidélité, l'historique des recherches faites sur internet, les relevés de compte bancaire, les courriels envoyés ou reçus, etc.)[7].

En revanche, cette obligation n'a pas trait aux données qui seraient générées de manière dérivée à partir de données fournies initialement par la personne concernée. Est ainsi concernée par cette exclusion la création d'un profil d'utilisateur par un algorithme, suite à l'extraction de données brutes concernant une personne physique ou même morale.

Échappent aussi à l'obligation de portabilité les données personnelles faisant l'objet d'une autre légalité que celle du consentement ou de l'exécution d'un contrat. Sont principalement impactées ici les données connaissant des prescriptions d'ordre public. Par exemple les banques n'ont pas à répondre aux demandes de portabilité concernant les opérations liées à la lutte contre le blanchiment d'argent.

Cette demande de transfert obéit à un certain formalisme. Cette demande doit ainsi être lisible par le matériel informatique et donc assez fréquemment utilisée. La technologie utilisée pour le transfert doit aussi garantir l'interopérabilité du traitement effectué. Il n'y a pas pour autant ici d'obligation de stricte similitude des formats de transferts, ils doivent juste être compatibles et s'adapter au secteur d'activité des organismes concernés.

7. *Le droit à la rectification ou à l'effacement des données personnelles :*

Les articles 16 et 17 du RGPD abordent les questions de la rectification et de l'effacement des données personnelles.

Le droit de rectification est concerné par l'article 16 du RGPD. Il permet à la personne physique ou morale concernée par les données personnelles en question de demander dans les meilleurs délais la rectification ou le complément de celles-ci. La principale condition de validité de cette démarche est d'estimer que ces données sont inexactes ou incomplètes. Reste à savoir aujourd'hui quels seront les moyens de la preuve de cette inexactitude ou du caractère incomplet La notion de meilleur délai sera également à préciser.

L'article 17 du RGPD a trait quant à lui au droit à l'effacement des données

personnelles. Il ne s'agit ni plus ni moins ici que de la consécration d'un droit à l'oubli numérique pour l'ensemble des internautes.

Le RGP liste six situations donnant lieu à un droit à l'effacement des données personnelles. Le premier cas est celui des données reconnues comme n'étant plus nécessaires quant aux finalités pour lesquelles elles ont été initialement collectées ou traitées. Sont ensuite concernées les données ayant trait à un retrait de consentement de la part de la personne physique ou morale ayant à l'origine autorisé le traitement desdites données. Ce cas de figure englobe aussi les données pour lesquelles il n'existe pas de fondements juridiques au traitement. Le troisième cas est celui ou la personne physique ou morale objet des données s'oppose à leur traitement en application de l'article 21, paragraphe 1 du RGPD. Sont concernées également ici les données à caractère personnel pour le traitement desquelles ne se manifeste pas un motif légitime et impérieux, d'ordre public par exemple. S'applique ici l'article 21 paragraphe 2 du RGPD. Le quatrième cas concerne les données à caractère personnel ayant fait l'objet d'un traitement illicite. La cinquième situation concerne les données à caractère personnel dont l'effacement est commandé par une disposition légale d'un État membre ou de l'Union européenne. Enfin le sixième droit à l'effacement concerne les données à caractère personnel ayant été collectées dans le cadre d'une offre de service de sociétés d'informations ayant trait aux enfants de moins de 16 ans. Les États membres ont ici une petite marge d'adaptation et pourront assouplir cette mesure en ramenant cette limite d'âge à 13 ans.

Les données objets de la demande d'effacement ont pu être rendues publiques via des moteurs de recherches ou même des fichiers de clientèles des plateformes de ventes (aux risques d'atteintes manifestes au respect de la vie privée). Peuvent être aussi ici impactés les fichiers publics révélant les noms de membres d'associations ou de mouvements, qu'ils soient politiques ou non.

Pour l'ensemble de ces cas et d'autres situations non référencées où des données à caractère personnel sont rendues publiques, le responsable de la plateforme concernée devra dans les meilleurs délais prendre toutes les mesures envisageables pour informer le responsable du traitement qu'une demande d'effacement a été enregistrée. Ce responsable devra alors lui-même procéder à la suppression desdites données ainsi que de leurs copies et reproductions, dans les meilleurs délais.

Existent enfin des données à caractère personnel pour lesquelles il n'existe pas de droit à l'effacement. Cinq cas sont ici listés par le RGPD. Le premier cas concerne les données à caractère personnel s'effaçant devant les impératifs des droits à la liberté d'expression et d'information. Le second concerne les traitements de données personnelles rendus obligatoires par le droit de l'Union européenne ou le droit d'un État membre, si ces textes imposent la conservation desdites données. Cette situation concerne également le cas où lesdites données personnelles sont conservées dans le but d'exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est alors investi le responsable du traitement. Le troisième cas de figure est celui où les données personnelles conservées ont trait à des motifs d'intérêt public concernant le domaine de la santé publique. Le quatrième cas est enfin celui de la conservation de données personnelles ayant trait à la conservation d'archives présentant un intérêt scientifique, historique, statistique ou plus simplement public. L'effacement de ces données est alors interdit s'il est de nature à rendre impossible ou à compromettre gravement la réalisation des objectifs de leur traitement. Enfin l'effacement des données à caractère personnel peut être interdit si le maintien de leur enregistrement est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.

8. *Le droit à la limitation du traitement des données à caractère personnel :*

Le droit à la limitation du traitement des données à caractère personnel survient dans l'un des quatre cas suivants prévus par le RGPD. La première situation est celle où l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel. Le second cas est celui où un traitement des données à caractère personnel est reconnu comme illicite avec une opposition de la personne concernée à l'effacement de celles-ci et lorsque cette même personne n'exige qu'un traitement limité desdites données. Le troisième cas concerne le responsable du traitement qui n'aurait plus besoin de conserver des données personnelles aux fins de leur traitement alors que celles-ci sont néanmoins nécessaires à la personne conservée, laquelle a besoin que lesdites données ne soient pas effacées à des fins de constatation, d'exercice ou de défense d'actes en justices. La quatrième et dernière situation est celle où la personne concernée par les données à caractère personnel s'est opposée à leur traitement en application de l'article 21 paragraphe 1. Cette personne peut demander une limitation du traitement des données à caractère personnel la concernant pendant la vérification de la légitimité des allégations d'un

responsable du traitement arguant de raisons légitimes pour conserver des données personnelles à l'encontre du souhait d'un effacement de celles-ci.

A suivre

1. Règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *« relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) »*, publié au JOUE du 4 mai 2016 L 119/1.
2. Directive n° 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *« relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données »*, publiée au JOUE du 23 novembre 1995 pp 0030-0051.
3. Parlement européen, résolution législative du 12 mars 2014 « sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », publiée au JOUE du 13 mars 2014.
4. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) », publié au JOUE du 4 mai 2016, L 119/1.
5. CJUE, 13 mai 2014, *« Google Spain et Google »*, arrêt ECLI:EU:C:2014:317.
6. CNIL, « Le droit à la portabilité en questions », rapport du 22 mai 2017.
7. Op Cit 6.