NOTE
relative à la **Protection des Données Personnelles (RGPD)**

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), paru au JOUE du 4 mai 2016.

C'est un texte qualifié d'historique, dont le champ d'application est très large. Ce texte, qui s'appliquera à tous les traitements existants, nécessite de se lancer dès à présent dans le chantier de la mise en conformité. Une nécessité d'autant plus impérieuse que les sanctions sont significativement alourdies (amende administrative de 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial).

La loi dite « Informatique et Libertés » (LIL) du 6 janvier 1978 (conçue pour la collecte d'informations de la part des Administrations) est devenue largement obsolète, en dépit de sa réforme de 2004, à l'heure du « Big data » mis en place par des opérateurs privés. Relevons que l'Union Européenne n'oblige pas les Etats membres à modifier leur législation nationale existante ; le choix de la France est néanmoins de modifier celle-ci et un projet de loi est en cours de discussion devant le Parlement.

Partant de l'idée que la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental, le Règlement se propose de protéger les personnes physiques à l'égard du traitement des données à caractère personnel les concernant (et leur transfert notamment hors Union Européenne) quel que soit leur nationalité ou leur lieu de résidence.

A retenir

Définitions de trois notions essentielles du Règlement RGPD :

- ***personne physique :*** le RGPD cherche à protéger les personnes physiques identifiée ou identifiable (par tous moyens) mais pas les personnes morales ; la collecte et le traitement des données personnelles de ces dernières – dénomination sociale, forme juridique, coordonnées – sont donc libres ;
- ***traitement de données :*** toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés (collecte, enregistrement, organisation, structuration, communication par transmission, diffusion, rapprochement, interconnexion, effacement, destruction) ;
- ***responsable du traitement :*** personne physique ou morale, autorité publique, service, organisme qui, seul ou avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.

Doivent, à ce titre, être particulièrement protégé le respect de la vie privée et familiale, du domicile et des communications, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique.

A retenir

Le Règlement vise à protéger la collecte des données personnelles auprès des personnes physiques dans le cadre de ce que l'on appelle l'économie participative mais aussi offrir une protection à la circulation de ces données dans et hors l'Union Européenne.

Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel.

A retenir

Le Règlement RGPD ne s'applique pas aux politiques relevant de la souveraineté des Etats membres (immigration, sécurité, asile, terrorisme, enquêtes et infractions pénales ni aux activités strictement personnelle ou domestique d'une personne physique même si les fournisseurs de réseaux sociaux – Facebook… - sont soumis au RGPD.

Le nouveau Règlement (dit « RGDP »), **entrera en vigueur à compter de mai 2018.**

A retenir

Si la loi actuellement en discussion devant le Parlement français n'est pas adoptée avant le 25 mai 2018, c'est le Règlement européen qui trouvera à s'appliquer automatiquement. Si la loi française est lacunaire sur certains points, c'est le RGPD qu'il conviendra d'appliquer à ceux-ci.
La loi réforme la loi « Loi Informatique et Libertés » ; elle se prononce sur les points laissés libres par le « RGPD » ; ainsi de l'âge du consentement des personnes qui est fixé, pour l'instant, à 15 ans.

Il s'applique à tout traitement de données à caractère personnel, automatisé ou non : il concerne donc la quasi-totalité des acteurs économiques (car qui ne manipule aucune donnée ?), y compris ceux situés à l'étranger dès lors qu'ils s'adressent à des personnes situées en Union Européenne.

A retenir

Le Règlement RGPD a clairement une portée extraterritoriale. Car s'il s'applique à tout opérateur (comme son sous-traitant) doté d'un établissement au sein de l'Union Européenne qui collecte et traite des données, il vise aussi tout opérateur qui bien que situé hors U.E. vise, par ses services, des personnes physiques situées dans l'U.E. (cela afin de pouvoir contrôler les opérateurs américains qui proposent leurs services en Europe sans cependant vouloir en appliquer les règles). L'on peut cependant douter de la possibilité des autorités nationales en charge du contrôle et des sanctions de véritablement opérer hors U.E.

Le Règlement soutient le même esprit que la directive 95/46/CE ou la LIL, à savoir une proportionnalité des démarches, mesures et garanties à mettre en place au regard du risque suscité par le traitement sur les libertés individuelles des personnes concernées.

A cet égard, son article 1er est particulièrement éclairant quant aux finalités poursuivies : « Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée sparence) ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ; 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, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

Pour garantir le traitement des données conformément au RGPD, une nouvelle fonction apparaît le Responsable du Traitement des Données (RT ou Data Protection Officer - DPO) ; il est responsable du respect des finalités ayant engendrées la collecte des données et est en mesure de démontrer que le RGPD est respecté (responsabilité) ».

L'article 6 du RGP, précise dans quels cas le traitement des données est licite :

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 ;

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 étant précisé que ce point f) ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

En principe, et sauf exception (notamment basées sur le consentement exprès) le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

A retenir

Dans le cas où le traitement des données repose sur le consentement, le responsable du traitement doit rapporter la preuve que celui-ci a bien été donné. La collecte du consentement doit se faire de manière claire et explicite (et pas noyée dans les CGV). Le consentement à un contrat n'équivaut pas au consentement de la collecte des données : il faut en recueillir deux distincts. Une fois donné, le consentement peut être retiré mais que pour l'avenir (le traitement des données déjà collectées demeure valable). Enfin, lorsque le consentement à recueillir est celui d'un enfant âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. La loi française pourrait varier sur ce dernier point. A suivre…

Pour mémoire, le consentement est défini par le RGPD comme toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Les droits des personnes dont les informations à caractère personnel ont été collectées ont été clarifiés et renforcés.

Au moment où les données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit un certain nombre d'informations (coordonnées RT-DPO, finalités de la collecte, informations quant à la conservation des données, droit d'accès, droit de correction, droit à l'oubli, droit de saisir une autorité publique d'une réclamation…).

Les personnes concernées par la collecte des données bénéficient :

- droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes (droit de rectification) ;

-le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, en présence de certains motifs (données plus nécessaires à la finalité qui les avaient justifiées, retrait du consentement, traitement illicite des données - droit à l'oubli) ;

- le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique: contestation de l'exactitude des données personnelles, traitement illicite des données… (droit à la limitation) ;

- le droit à la portabilité des données c'est-à-dire 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 sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle (portabilité) ;

- le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant (droit d'opposition).

A retenir

Le Règlement RGPD tente de trouver un équilibre entre liberté de collecter et d'exploiter des données personnelles par les opérateurs économiques et la légitime protection de ceux qui fournissent plus ou moins consciemment ces données.

En synthèse, la « LIL » distingue à ce jour quatre grandes catégories de traitements :

- les traitements n'impliquant aucun risque (dispense de démarches préalables) ;
- les traitements courants non susceptibles de présenter un risque (procédures simplifiées) ;
- les traitements présentant un faible risque ou du moins modéré (déclaration normale) ;
- les traitements présentant un risque élevé (autorisation préalable ou procédure d'avis).

Prônant la responsabilisation des acteurs, le Règlement tend à distinguer deux grands types de traitements et non plus quatre (simplification) :

- les traitements qui, « compte tenu de la nature, de la portée, du contexte et des finalités du traitement,[sont] susceptible[s] d'engendrer un risque élevé pour les droits et libertés des personnes physiques » (traitements soumis à une obligation de réalisation d'une analyse d'impact et, le cas échéant, d'une consultation préalable de l'autorité de contrôle – art. 35) ;

- les autres traitements.

Une mise en conformité des pratiques existantes s'impose ou s'imposera à brève échéance.

Dans cette perspective, trois points doivent retenir particulièrement l'attention des opérateurs :

1°) réviser les mentions d'information et les modalités de recueil de consentement

Le Règlement dispose dès son préambule (Consid. n° 40) que « pour être licite, le traitement de données à caractère personnel devrait être fondé sur le consentement de la personne concernée ou reposer sur tout autre fondement légitime(…) ». La Loi Informatique et Libertés (LIL) étant muette sur ce point, jusqu'à présent, chaque responsable, à moins de bénéficier des exceptions au recueil de consentement prévues à l'article 7 de la LIL, l'obtenait selon la méthode qui lui convenait le mieux.

Désormais (Consid. n° 32), « Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques (…) ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité ».

Dès lors, il semblerait que tout Responsable devrait en principe - selon nous - réaliser, d'ici l'entrée en application du Règlement (c'est-à-dire d'ici 2018), une nouvelle communication auprès des personnes concernées afin d'informer les personnes sur les nouvelles mentions obligatoires et d'obtenir un consentement conforme aux prescriptions du Règlement, le cas échéant.

2°) identifier le nouveau régime applicable

L'ensemble des traitements existants mis en œuvre à la suite d'une décision d'autorisation de la CNIL, ou d'une procédure d'avis, sont désormais soumis à la réalisation d'une étude d'impact. Quant à ceux mis en œuvre suite à la réalisation d'une norme simplifiée ou d'une déclaration normale, ils doivent être analysés afin de vérifier si, en application du Règlement, ils sont soumis à cette même étude d'impact. Précisons que l'article 35, 3 du Règlement dispose que l'analyse d'impact relative à la protection des données est, en particulier, requise dans les cas suivants :

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatise, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;

- le traitement à grande échelle de catégories particulières de données visées à l'article 9, ou de données à caractère personnel relatives à des condamnations pénales et a des infractions ;

- ou la surveillance systématique à grande échelle d'une zone accessible au public.

Relevons pour finir sur ce point que, normalement, la CNIL a, dans la perspective de l'adoption du Règlement, déjà sensibilisé les responsables du traitement des données.

3°) mettre à niveau les mesures de sécurité

La « LIL » ne définit pas la nature des mesures de sécurité que doivent mettre en place les Responsables ainsi que les sous-traitants (ST). Bien sûr, la doctrine de la CNIL a dégagé quelques mesures de protection générales, notamment prévues dans les annexes « sécurité » des formulaires de la CNIL. Le Règlement confère une valeur réglementaire à certaines mesures. Ainsi, dans la mesure où le RT et le ST restent libres dans le choix des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques », le Règlement énumère les mesures suivantes qui doivent être mises en œuvre « selon les besoins», en fonction du degré de probabilité et de gravité du risque (art. 32-1) :

- la « pseudonymisation » ;
- le chiffrement ;
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes (capacité d'un système à absorber une perturbation en continuant de fonctionner) ;
- les moyens permettant de rétablir la disponibilité des données et leur accès dans des délais appropriés en cas d'incident physique technique ;
- une procédure de tests, analyse, évaluation régulière de l'efficacité des mesures de sécurité.

En résumé, l'entrée en vigueur du RGPD va devoir conduire à une adaptation de la loi « Informatique et Libertés ». Précisément, sept points doivent retenir l'attention :

- le RGPD a un champ territorial plus étendu que ce qui était jusqu'à présent prévu ; en effet, le règlement 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 ;

- de nouvelles données sont explicitement considérées comme sensibles (par exemple, données biométriques, génétiques, données concernant la santé) ;

- si les principes directeurs qui sous-tendent le RGPD ne sont pas inconnus de la LIL, ceux-ci se trouvent confirmés ;

- trois nouveaux droits de la personne concernée font leur apparition : droit de rectification, droit à l'oubli et droit à la portabilité des données ;
- suppression des formalités préalables à la mise en œuvre des traitements (déclarations et autorisations auprès de la CNIL se trouvent supprimés) au profit de mesures dites d'accountability c'est-à-dire de conformité avec des mesures techniques et opérationnelles permettant de garantir que le traitement est effectué conformément à la réglementation mise en place par le RGPD ;

- modification du statut de la CNIL et des sanctions qui peuvent être infligées ;

- modification des règles relatives au transfert hors U.E. des données personnelles collectées.