DIGITALISATION DU TRAVAIL – DES SOURIS ET DES HOMMES

1. Accéder aux données personnelles et contrôler leur gestion

De la souveraineté de l'individu sur ses données personnelles à l'heure du RGPD

par Marie-France MAZARS,
Doyen honoraire de la Cour de cassation,
Vice-président délégué de la CNIL

PLAN

Pour bien comprendre la problématique de la protection des données à caractère personnel, il faut souligner que l'enjeu n'est pas la donnée, mais la souveraineté de l'individu sur ses données à caractère personnel. Il s'agit de protéger les personnes à l'égard du traitement de leurs données personnelles. L'article 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés énonce que « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique du 7 octobre 2016 précise que « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ».

Le règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016, connu sous l'acronyme de RGPD, apporte une conception autonome de la protection des données personnelles en se référant à l'article 8 de la Charte des droits fondamentaux de l'Union européenne aux termes duquel :
« 1- Toute personne a droit à la protection des données personnelles la concernant.
2- Ces données doivent être traitées loyalement à des fins déterminées et sur la base du consentement de la personne ou en vertu d'un autre fondement légitimé prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3- Le respect des règles est soumis au contrôle d'une autorité indépendante ».

Au sein de l'entreprise ou de l'organisme et dans les relations de travail, la gestion des données personnelles n'est pas seulement l'affaire de l'employeur. Les dispositifs mis en œuvre doivent permettre aux salariés de maîtriser leur usage.

I. Nouvelle architecture des textes

La gestion par l'entreprise des données à caractère personnel était soumise aux dispositions de la loi du 6 janvier 1978, modifiée par la loi du 6 août 2004 à la suite de la transposition de la directive 95/46/CE du 24 octobre 1995. Mais, depuis le 25 mai 2018, date de l'entrée en vigueur du RGPD, il convient de se référer aux dispositions du droit de l'Union européenne, ainsi qu'à la loi du 6 janvier 1978 et à celle du 7 octobre 2016 qui contiennent des dispositions novatrices.

Le règlement européen, qui fixe les principes, a laissé des marges de manœuvres aux États membres, qui doivent, par ailleurs, réorganiser leur autorité de contrôle (la CNIL en France) pour les mettre en conformité avec les nouvelles dispositions. Une loi n° 2018-493 du 20 juin 2018 a donc modifié certaines dispositions de la loi du 6 janvier 2018. Son article 32 habilite le Gouvernement à prendre par ordonnance les mesures nécessaires pour assurer « *une cohérence rédactionnelle, harmoniser l'état du droit, remédier aux éventuelles erreurs et omissions résultant de la présente loi et abroger les dispositions devenues sans objet* ». Cette ordonnance est en cours de rédaction. Elle apportera des modifications à la loi de 1978 et sera applicable à la date d'entrée en vigueur du décret d'application qui, lui aussi, est en cours de rédaction. On peut envisager une stabilisation des textes au cours de l'année 2019 (1).

Le changement essentiel, qui va impacter les entreprises, réside dans la nouvelle logique qu'institue le RGPD. Ce sont les acteurs eux-mêmes qui ont la charge d'assurer la conformité de leurs traitements informatiques aux normes de la protection des données et qui en sont responsables. Il n'y a plus de déclaration préalable à la CNIL ou de demande d'autorisation.

Le règlement prévoit que le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées afin de pouvoir démontrer que le traitement est effectué conformément au règlement. Pour certains traitements comportant des risques pour les droits et libertés, le responsable du traitement devra effectuer une étude d'impact sur la vie privée.

II. La mise en place des mesures techniques et organisationnelles dans les entreprises

A. Le registre des activités de traitement prévu par l'article 30 du RGPD

Ce registre remplace les déclarations de traitement qui devaient être faites à la CNIL. Il servira à l'information au sein de l'entreprise et à la CNIL dans l'exercice de sa mission de contrôle.

Il doit comporter les informations suivantes :
– la ou les finalités du traitement ;
– les catégories de personnes concernées et les catégories de données ;
– les catégories de destinataires ;
– les transferts de données hors de l'Union européenne ;
– les délais prévus pour l'effacement des données ;
– une description des mesures de sécurité.

Si ce registre n'est obligatoire que dans les entreprises de plus de 250 salariés, il faut souligner qu'il s'impose également dans celles où :
– les traitements sont susceptibles de comporter des risques pour les droits et libertés des personnes ;
– les traitements sont réguliers (non occasionnels) ;
– les traitements portent sur des catégories particulières de données : données sensibles ou données d'infractions ou de condamnations.

Ces critères n'étant pas cumulatifs, l'obligation de tenir un registre concerne la plupart des entreprises.

B. Le délégué à la protection des données (DPD ou DPO *data protection officer*)

Nous connaissions, depuis 2005, une telle institution en France : le correspondant informatique et libertés (CIL).

La désignation d'un DPO est obligatoire ou facultative. Elle est obligatoire pour les organismes publics, à l'exception des juridictions.

Elle l'est également pour les organismes privés :
– dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle;
– dont les activités de base les amènent à traiter des données dites sensibles ou relatives à des condamnations pénales ou des infractions.

(1) Cette ordonnance est intervenue le 12 décembre 2018. Elle entrera en vigueur en juin 2019, en même temps que le décret d'application de la loi « Informatique et Libertés ». Actuellement et dans cette attente, les dispositions actuelles de la loi « Informatique et Libertés », dans sa version modifiée le 22 juin 2018, sont seules applicables.

Ses fonctions et ses missions sont précisément définies par le RGPD.

Les organismes et les entreprises ont pris conscience de l'intérêt de désigner un DPO. Alors que nous avions auparavant 5.000 CIL, nous avons actuellement plus de 15.000 DPO, dont les coordonnées ont été communiquées à la CNIL.

On peut considérer qu'il s'agit d'un véritable métier. D'ores et déjà, des dispositions concernant leur formation et leur certification ont été prévues. La CNIL a adopté un référentiel concernant cette certification (2).

Sur ces deux points déjà, le changement devrait être visible dans les entreprises.

III. Obligation pour les employeurs, responsables de traitement, de recenser tous les traitements en place et de se poser les questions relatives à leur conformité

Avant d'aborder, sur le fond, les grands principes du RGPD, on peut citer quelques exemples des traitements informatiques ou non informatisés les plus usuels :
– opérations de recrutement ;
– annuaires du personnel ;
– dossiers personnels tels que recrutement, historique de carrière, rémunération, évaluation des compétences (entretiens annuels, notations…, dossier disciplinaire) ;
– réseaux sociaux d'entreprises ;
– contrôle de l'utilisation d'internet (filtrage des sites non autorisés, exigences de sécurité et messages) ;
– vidéosurveillance sur les lieux du travail ;
– gestion de la téléphonie ;
– géo-localisation des véhicules ;
– utilisation de badges ou de dispositifs biométriques.

Quels sont les points à vérifier pour évaluer la conformité d'un traitement aux dispositions du RGPD ?

A. La licéité du traitement au regard de l'objectif poursuivi, quelle base légale ? (article 6 du RGPD)

Consentement des personnes ? Respect d'une obligation légale ? Exécution d'un contrat ? Intérêt légitime du responsable de traitement ou d'un tiers ?

B. La ou les finalités poursuivies par le traitement

Les traitements habituels RH peuvent avoir, par exemple, pour finalités :
– le recrutement des personnels ;
– la gestion administrative des personnels ;
– la gestion des rémunérations et l'accomplissement des formalités y afférentes ;
– la mise à disposition des personnes d'outils informatiques ;
– l'organisation du travail ;
– la gestion des carrières et de la mobilité ;
– la formation des personnels.

D'autres traitements utilisant des nouvelles technologies ont souvent les finalités suivantes :
– surveillance des locaux, des véhicules et du matériel (vidéosurveillance, géo-localisation) ;
– prévention de fuites de données à l'extérieur de l'entreprise (*Data Loss Prevention*, système qui permet d'analyser les réseaux internes, les postes de travail et les points de sortie des réseaux pour détecter ou prévenir une perte de données).

C. Une collecte licite, loyale et transparente des données pour des finalités explicites, déterminées et légitimes, limitées à ce qui est nécessaire au regard de ces finalités (principe de minimisation des données)

L'article 5 du RGPD énonce ces principes (qui sont ceux qui fondent la protection des données personnelles de la loi de 1978) qui, dans la mesure où les entreprises sont tenues, sous peine de contrôles et de sanctions, de prendre en charge la conformité, devraient aboutir à une réduction drastique de la quantité et de la nature des données traitées.

Ainsi, les risques de fuite ou de mauvaise utilisation des données s'en trouveront-ils diminués.

En résumé, toute donnée collectée et utilisée devra être justifiée au regard de la finalité du traitement (par exemple, le traitement informatique ne devra pas collecter l'appartenance syndicale. Mais il pourra collecter cette donnée s'il s'agit d'un traitement utilisé

(2) Délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO). Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO).

pour calculer et payer les heures de délégation du salarié représentant du personnel.)

Par ailleurs, le contrôle de proportionnalité doit être opéré entre l'objectif poursuivi et le moyen choisi pour l'atteindre au regard de l'impact sur la vie privée et les libertés du salarié. On trouve un exemple de l'effectivité d'un contrôle de proportionnalité dans celui qu'effectuait la CNIL pour refuser l'autorisation du dispositif biométrique ou d'un système de géo-localisation pour contrôler les horaires de travail du salarié. Ces techniques sont considérées comme intrusives et l'employeur peut utiliser d'autres moyens, moins attentatoires aux libertés des personnes, pour atteindre cet objectif.

D. La durée de conservation

Les données ne peuvent être conservées que le temps nécessaire à l'accomplissement de l'objectif poursuivi. La durée de conservation doit être prévue dès la création du fichier et des modalités de suppression automatique doivent être mises en place.

Certains délais suivront les dispositions du Code du travail (ceux de l'article D. 3171-16, qui prévoit que le décompte des horaires de travail du salarié doit être conservé pendant un an ou pendant 3 ans pour les salariés intéressés par des conventions de forfait ou, par exemple, lorsqu'un salarié quitte l'entreprise, son adresse électronique doit être supprimée des fichiers).

L'employeur devra, en tout état de cause, pouvoir justifier du délai de conservation qu'il a retenu.

IV. Les employeurs contraints de mettre en place des mesures assurant la transparence des informations et des communications et des modalités d'exercice des droits des salariés (articles 12, 13 et 14 du RGPD)

Le RGPD a apporté un changement de taille dans l'amélioration de la transparence. Il définit les informations à fournir pour chaque traitement.

Les personnes concernées sont informées de ce que l'on fait de leurs données et des droits qu'elles détiennent, **information qui doit être « *claire, intelligible et aisément accessible* ».**

Aux informations qui devaient être fournies lors de la collecte des données, selon l'article 32 de la loi de 1978 (3), s'ajoutent celles relatives aux coordonnées du responsable du traitement, à la base juridique du traitement, au droit de retirer son consentement, à celui de porter plainte auprès de la CNIL, aux coordonnées du DPO et à l'existence d'une prise de décision automatisée.

Lorsque les données sont recueillies de manière indirecte (auprès de tiers) ou lorsqu'elles proviennent de sources accessibles au public, le RGPD impose l'information, dans un délai raisonnable ne pouvant pas dépasser le délai d'un mois.

On rappellera que l'article L. 1224-4 du Code du travail dispose que **« aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ».**

L'employeur doit apporter la preuve et la qualité de l'information, quelles que soient les modalités de cette information (affichage, note, mail avec accusé de réception).

Corollaire de l'obligation d'information, **le droit d'accès** permet à toute personne d'obtenir communication des caractéristiques du traitement et des données personnelles traitées (article 15 RGPD).

On rappellera simplement que toute personne peut interroger l'employeur responsable de traitement.

Les droits d'opposition, de rectification ou d'effacement existaient dans notre loi de 1978 et étaient exercés.

Le RGPD a institué un nouveau droit qui peut s'avérer très utile : le **droit à la limitation** (article 23 du RGPD). La personne qui exerce son droit à la limitation demande que ses données cessent d'être traitées (soient gelées) le temps de la vérification. Par exemple, le salarié exige que son employeur conserve les images enregistrées via le dispositif de vidéosurveillance afin de pouvoir les utiliser dans le cadre d'un contentieux**.** Cette possibilité est importante, car la durée de conservation des images de la vidéosurveillance est, en général, de quelques jours et au maximum d'un mois.

(3) Identité du responsable de traitement ; Finalité poursuivie ; Caractère obligatoire ou facultatif des réponses ; Destinataires ou catégories de destinataires des données ; Droit de définir des directives sur le sort des données en cas de décès ; Durée de conservation des données traitées ou critères permettant de définir la durée.

La CNIL accompagne les employeurs dans la mise en place de la conformité à ces règles de protection des données personnelles. Comme la loi de 1978 modifiée le lui permet, elle publie des référentiels. Celui concernant la gestion des ressources humaines est en préparation et fera l'objet d'une consultation publique. Il y en aura d'autres, notamment un référentiel concernant les enregistrements des conversations téléphoniques, la vidéosurveillance et la géo-localisation.

Elle a également publié la liste des traitements ne nécessitant pas la réalisation d'analyses d'impact. Parmi ces traitements figurent ceux relatifs à la gestion administrative des salariés.

Enfin, elle a élaboré un projet de règlement-type relatif aux dispositifs biométriques de contrôle d'accès aux lieux de travail, lequel a été soumis à consultation publique (4).

V. Obligation pour les responsables de traitement d'analyser les risques pour la vie privée que représente l'utilisation du profilage et des algorithmes pour le recrutement, l'évaluation et le suivi des parcours professionnels

L'article 4-4 du RGPD définit le profilage comme « *tout forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne*. » Et l'article 22 dispose que « *la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant les effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ».

De tels traitements ne pourront avoir pour base légale que le consentement du salarié. Les instances représentatives du personnel seront nécessairement consultées. Les responsables du traitement (ou leur sous-traitant) seront tenus d'effectuer une analyse d'impact relative à la protection des données (AIPD) (5).

Par ailleurs, il sera essentiel de veiller à la fiabilité des données sur lesquelles va fonctionner l'algorithme et aux critères retenus pour définir l'algorithme. Pour illustrer le danger de traitements reposant sur le seul fonctionnement d'un algorithme, on donne le plus souvent l'exemple suivant. En avril 2016, Amazon avait exclu de ses services « livraison en un jour » certains quartiers peuplés majoritairement de populations défavorisées de Boston, Atlanta, Chicago, Dallas, New York et Washington, car, selon une analyse de ses données, les quartiers en question ne généraient pas de profit pour l'entreprise. Si l'objectif n'était pas d'exclure de ses services des zones où la population était majoritairement noire, le résultat du fonctionnement de l'algorithme avait cette conséquence : les citoyens noirs avaient deux fois moins de chances que les blancs de vivre dans les zones desservies par le service d'Amazon en question.

Le paramétrage des algorithmes peut avoir pour conséquence de reproduire des biais ou des discriminations. C'est la raison pour laquelle il faudra veiller aux critères retenus pour la détermination de l'algorithme.

***

Les changements induits par le RGPD vont apporter aux droits des salariés des organismes publics et privés une meilleure protection et davantage de transparence et de sécurité.

Les acteurs parmi lesquels, dans les relations de travail, les représentants du personnel et les organisations syndicales, doivent se saisir de l'opportunité de l'installation, dans les entreprises et les organismes, d'outils destinés à une meilleure gestion des données personnelles et y participer.

L'un des outils qui pourrait être mobilisé est celui de l'action de groupe (*class action*), qui peut être exercée par les organisations syndicales de salariés ou de fonctionnaires représentatives aux fins de cessation du manquement aux obligations du responsable du traitement ou de voir engager sa responsabilité du fait du dommage causé par le manquement (6).

Marie-France Mazars

(4) Le règlement type a été adopté par une délibération du 10 janvier 2019.

(5) Le site de la CNIL donne une information complète et un outil permettant de réaliser l'AIPD.

(6) Art. 80 du RGPD ; art. 43 ter de la version actuelle de la loi « Informatique et Libertés ».