Analyses

IP/IT

Un an après le RGPD – Chronique d'un droit dépoussiéré

Le Règlement européen sur la protection de données (RGPD), entré en vigueur le 25 mai 2018, est venu réformer le droit des données personnelles en instaurant de nombreux principes jusqu'alors peu considérés par le législateur français et sa vieillissante loi Informatique et Libertés de 1978[1] et par le législateur européen dans la Directive européenne de 1995[2].

Par Mélanie Erber, associée,

Ce faisant, il a bouleversé le comportement des entreprises, soucieuses de se mettre en conformité avec de nouvelles normes qui accordent désormais à l'utilisateur des droits sur ses données à caractère personnel et imposent des obligations aux entreprises quant au traitement de ces données. Entre mythe et réalité, cette année écoulée permet de dresser un bilan du texte qui a engendré de nombreuses adaptations pour les entreprises traitant de la donnée, et un grand engouement pour les personnes dont les données ont été collectées.

Un texte mais plusieurs lois

La publication du RGPD le 25 mai 2018 a eu pour effet d'abroger la Directive européenne de 1995, devenue obsolète face au développement d'Internet et des réseaux sociaux et jusqu'alors le seul apport européen en matière de données personnelles. Au-delà des technicités d'Internet non prévues il y a vingt-cinq ans par le législateur européen, cette dernière faisait preuve d'une difficulté pratique : elle n'avait pas été transposée dans tous les Etats membres, si bien qu'en pratique, ces derniers avaient besoin d'une uniformisation du droit en vigueur.

Le RGPD répond à cette exigence puisqu'il a le mérite d'unifier le droit européen. Néanmoins, le texte laisse quelques libertés d'interprétation souveraine aux Etats membres dans certains articles.

C'est la raison pour laquelle, le 21 juin 2018, la France – traditionnellement pionnière en matière de protection des personnes – a promulgué une loi venant supplanter la poussiéreuse loi Informatiques et Libertés de 1978 et dans laquelle on retrouve notamment une transposition de la Directive européenne 2016/680 sur les traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, ainsi que de nombreux points traités par le RGPD et des précisions relatives aux quelques rares notions imprécises du texte.

Parmi ces apports, les dispositions relatives aux mineurs, déjà présentes dans le RGPD, ont été renforcées. En effet, le RGPD laisse aux Etats membres la possibilité d'abaisser l'âge de la majorité numérique jusqu'à 13 ans : à compter de cette majorité, le consentement peut être recueilli directement auprès du mineur concerné et non par l'intermédiaire de ses parents. Face aux dérives des réseaux sociaux, le législateur français a prévu que la majorité numérique serait fixée à 15 ans en France : un recueil du consentement du titulaire de l'autorité parentale est donc nécessaire en dessous de cet âge.

A ce texte s'ajoutent également l'ordonnance du 13 décembre 2018 qui achève la mise en conformité du droit national au RGPD et de nombreux décrets d'applications, comme celui du 21 avril 2019 autorisant l'employeur à faire usage du numéro de sécurité sociale[3].

Enfin, le projet de Règlement sur l'e-privacy[4] vient encadrer l'utilisation des métadonnées, des cookies, des adresses IP, de données de géolocalisation, etc. toujours dans le but de renforcer la protection de la vie privée de l'internaute. Si ce texte devait entrer en vigueur en même temps que le RGPD, il est retardé du fait de puissants lobbyings à Bruxelles, inquiets d'une privation de liberté sur ces données, véritables mannes financières pour les acteurs du net.

Ce sont tant d'instruments législatifs, chapotés par le RGPD mais qu'il convient de manier avec précaution les uns à la lumière des autres.

Nouveaux mécanismes instaurés par le RGPD

Le principe d'«accountability» – ou de responsabilité – est la clé de voûte du RGPD. Les entreprises sont amenées à devoir désormais mettre en œuvre des mécanismes et procédures internes pour démontrer à tout instant qu'elles agissent en respect des règles de protection des données personnelles, responsabilisant ainsi les acteurs en présence.

C'est d'ailleurs à ce titre que les formalités de déclaration préalable auprès de la CNIL ont été suppri-

mées au profit des obligations notamment de tenue d'un registre de traitement des données ou encore de désignation d'un délégué à la protection des données personnelles (DPO, pour Data Protection Officer) qui pèsent sur le responsable de traitement.

Pour faire face à ces obligations, de nombreuses entreprises ont préféré avoir recours à un DPO, même s'il convient de rappeler que ce dernier n'est obligatoire que dans certains cas limitatifs[5]. Le RGPD renvoie aux législations nationales pour encadrer la désignation et qualification du DPO, ce que le législateur français n'a pas étayé dans la loi du 21 juin 2018.

Le principe du consentement a été aussi considérablement revisité, si bien que les entreprises, frileuses de sanctions inopinées, recueillent désormais tous azimuts depuis un an le consentement de chaque personne pour pouvoir continuer le traitement sur des données pourtant collectées souvent licitement !

Pour rappel, un traitement de données personnelles est licite s'il respecte une des six bases légales énoncées par l'article 6 du RGPD. Le consentement n'est qu'une des six bases légales. Aussi, le traitement est-il licite s'il repose par exemple sur un texte légal, sur l'exécution d'un contrat ou encore sur la poursuite d'un intérêt légitime.

La notion d'intérêt légitime, trop floue pour être utilisée de façon sereine par les responsables de traitement pour s'affranchir du consentement, a fait l'objet de nombreux débats doctrinaux depuis un an et a récemment été précisée par le Conseil d'Etat[6] à la lumière de l'article 21 du RGPD qui précise que «la personne concernée a 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». Pour la Haute Cour, les motifs légitimes s'entendent de motifs «tenant de manière prépondérante à sa situation particulière». Autant dire que ces précisions ne permettent pas de rassurer les responsables de traitement, tant elles restent en pratique trop floues à interpréter.

Un an de sanctions CNIL

Parmi les mesures phares du RGPD, ce dernier a prévu une augmentation des montants des sanctions en cas de non-respect des dispositions du RGPD pour le responsable de traitement ou ses sous-traitants, allant jusqu'à 2 % ou 4 % du chiffre d'affaires de l'auteur de l'infraction.

La CNIL dont le pouvoir de sanction a été renforcé depuis l'entrée en vigueur du RGPD a infligé à de nombreuses entreprises des sanctions pécuniaires, sans pour autant atteindre les millions annoncés et craints.

A titre d'exemple, en décembre 2018, la CNIL a prononcé à l'encontre de Bouygues Telecom une sanction pour un montant de 250 000 euros[7] et à l'encontre de Uber une sanction de 400 000 euros[8] pour avoir toutes deux manqué à leur obligation de sécurité et confidentialité des données.

Exception notable en la matière, le 21 janvier 2019, Google a été condamnée à l'amende record et exemplaire de 50 millions d'euros pour de nombreux manquements de la société depuis de nombreuses années quant aux données personnelles des Européens[9].

Corollaire du RGPD, la CNIL signale que l'intérêt collectif pour les données personnelles s'est accru avec l'entrée en vigueur du RGPD, puisque le nombre de plaintes déposées à la CNIL est passé de 11 077 en 2018 contre 8 300 en 2017.

La CNIL a aussi émis de nombreuses mises en demeure à l'encontre de sociétés, qui après explications de ces dernières sur les infractions reprochées, ont été clôturées pour la plupart par la CNIL.

De façon plus globale et pour accompagner les entreprises, la CNIL publie des délibérations visant à aider ces dernières dans la gestion de leurs données personnelles, en toute conformité avec le RGPD. A titre d'exemple, elle vient de publier un règlement type portant sur la biométrie au travail[10] dans le but d'aider des employeurs dans la mise en place de ces dispositifs de contrôle.

Ainsi, si le chemin vers une totale conformité est laborieux au vu de l'opacité qui règne encore sur certaines obligations instaurées par le RGPD, il reste pour le moins possible à condition de mettre en place en interne des mécanismes visant cette conformité. ■

et Sacha Bettach, avocate, Coblence & Associés

1. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
2. Directive n°95/46/CE, 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.
3. Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire.
4. Proposition de Règlement du parlement européen et du conseil 2017/0003 concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement vie privée et communications électroniques), le 10 janvier 2017.
5. Article 37 à 39 du RGPD
6. Conseil d'Etat, 10e et 9e chambres réunies, 18 mars 2019, n° 406313.
7. Délibération n° SAN-2018-012 du 26 décembre 2018.
8. Délibération n° SAN-2018-011 du 19 décembre 2018.
9. Délibération n° SAN-2019-001 du 21 janvier 2019.
10. Délibération n°2019-001, 10 janvier 2019