RGPD : LE TEMPS DES SANCTIONS

« Avec la réception et la transmission simultanées, ce fut la fin de la vie privée » (Georges Orwell, roman 1984) : c'est pour éviter la réalisation de ce type de prophétie que sont édictées des normes telles que le Règlement Général sur la Protection des Données européen, applicable depuis le 25 mai 2018 - ou encore quatre décennies plus tôt la loi française du 6 janvier 1978 Informatique et Libertés, toujours en vigueur même si amplement modifiée depuis, en dernier lieu précisément pour intégrer le RGPD.

Ces textes normatifs n'ont toutefois d'intérêt que s'ils sont réellement suivis d'effet ; si l'on peut à cet égard compter sur un phénomène d'opportunité que peuvent y voir les responsables de traitements de données pour communiquer sur leur mise en conformité RGPD vis-à-vis des personnes concernées (clientèle, abonnés, citoyens...), l'efficacité d'une telle réglementation se mesure également nécessairement à l'aune des sanctions qu'elle est susceptible de générer en cas de contravention.

À cet effet le spectre des sanctions prévues par le nouveau texte RGPD a été étendu (1), et leurs premières applications françaises ont d'ores et déjà été rendues par la CNIL (2).

1. SANCTIONS APPLICABLES

Tout d'abord en termes de procédure, la CNIL peut engager des contrôles :
- sur les plaintes qui lui sont adressées, lesquelles sont en constante augmentation depuis l'entrée en vigueur du RGPD : au nombre de 11.077 en 2018 selon son rapport annuel, soit + 32,5 %,
- ou parce que la CNIL décide de se saisir d'un cas particulier, sachant que les thématiques de contrôle annoncées pour 2019–2020 sont : le respect du droit des personnes concernées, le traitement des données des mineurs et la répartition des responsabilités entre les organismes et leurs sous-traitants.

Les modalités de ce contrôle par la CNIL ont été renforcées, pouvant désormais prendre quatre formes différentes, le cas échéant de manière cumulative (art. 19 de la LIL modifiée) : contrôle sur place, sur convocation, en ligne et/ou sur pièces ; précisons en outre que le 31 janvier 2019, la DGCCRF et la CNIL ont signé un nouveau

Julie GRINGORE

protocole de coopération afin de renforcer leur collaboration et de l'adapter aux nouveaux enjeux numériques.

Ensuite sur les sanctions elles-mêmes, la CNIL peut - en sa formation restreinte dont les décisions relèvent du Conseil d'État (art. 20 de la LIL modifiée) :
- prononcer un rappel à l'ordre,
- enjoindre de mettre le traitement en conformité ou de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte,
- limiter temporairement ou définitivement un traitement, ou suspendre les flux de données,
- prononcer une amende administrative.

En ce qui concerne plus précisément cette dernière catégorie de sanction constituée par les amendes administratives, plusieurs critères interviennent dans la détermination de leur montant ; ainsi :
- la nouvelle réglementation a fait passer leur plafond de 3 millions à 20 millions d'euros, ou 4 % du chiffre d'affaires annuel mondial (le montant le plus élevé des deux pouvant être retenu) ;
- la CNIL est tenue de prendre en compte, dans la détermination du montant de l'amende, les critères de l'article 83 du RGPD, à savoir notamment « la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage » ;
- des lignes directrices du CEPD (Contrôleur européen de la protection des données, anciennement G29) ont été prises pour harmoniser les pratiques des différentes autorités de contrôle nationales et ainsi accroître la sécurité juridique des responsables de données au niveau européen ; les institutions nationales peuvent elles-mêmes, à leur niveau, édicter leurs propres lignes directrices, ainsi que l'a d'ores et déjà fait la première l'autorité de contrôle néerlandaise selon publication du 14 mars 2019.

Précisons enfin qu'à ces sanctions administratives peuvent s'ajouter :
- des publications des condamnations prononcées par la CNIL, ce qui peut évidemment ternir l'image de l'entreprise concernée en termes de sécurité et de confiance vis-à-vis de ses clients ou usagers ;
- des sanctions pénales en application des articles L. 226–16 et s. du Code pénal, disposant notamment que « le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300.000 € d'amende ».

2. SANCTIONS APPLIQUÉES

Si l'on fait le point sur les sanctions prononcées à l'échelle européenne, il peut être noté qu'en application de la nouvelle réglementation RGPD :
- c'est l'autorité de contrôle portugaise qui a été la première à prendre une décision en date du 19 octobre 2018, condamnant un hôpital à 400.000 € d'amende notamment pour violation des principes d'intégrité, de confidentialité et de limitation d'accès aux données concernées ;
- en termes de quantum, c'est la CNIL française (suivie de l'Allemagne) qui a prononcé les sanctions les plus lourdes ; au jour de la rédaction des présentes trois décisions, exposées ci-dessous, ont été prises par l'autorité de contrôle française en application des nouvelles dispositions RGPD.

En premier lieu la société Google a fait l'objet d'une condamnation en date du 21 janvier 2019 - actuellement pendante devant le Conseil d'État sur recours de la société.

Deux manquements sont essentiellement sanctionnés par la CNIL dans cette affaire, au titre de l'information et du consentement des usagers :

- en ce qui concerne les informations délivrées aux utilisateurs, la CNIL considère qu'elles ne répondent pas « aux objectifs d'accessibilité, de clarté et de compréhension » fixés par l'article 12 du RGPD : d'une part celles-ci sont « excessivement éparpillées dans plusieurs documents... un tel choix ergonomique entraînant une fragmentation des informations », d'autre part leur caractère imprécis et incomplet est considéré comme d'autant plus grave que « *les traitements de données mis en œuvre par le responsable de traitement sont particulièrement massifs et intrusifs* » ;
- en ce qui concerne le consentement des usagers, celui-ci est considéré comme étant insuffisamment éclairé et univoque dès lors que l'utilisateur doit accepter « en bloc l'ensemble des traitements de données à caractère personnel », et que « les paramètres de son compte... sont tous pré-cochés par défaut... la possibilité laissée aux utilisateurs de paramétrer leur compte ne se traduit pas non plus, dans ce cas de figure, par un acte positif ayant pour objet de recueillir le consentement ».

En termes de condamnation, la CNIL souligne « la nature particulière des manquements relevés » et « le nombre de personnes concernées » (27 millions d'utilisateurs en France) pour motiver les sanctions prononcées, à savoir :
- 50 millions d'euros d'amende administrative, faisant ainsi jouer le plus haut des deux plafonds correspondant à 4 % du chiffre d'affaires mondial de la société (et non pas seulement le premier plafond fixé à 20 millions d'euros par les textes),
- une mesure complémentaire de publicité « sur le site de la CNIL et le site de Légifrance » (dont l'anonymisation prévue à l'expiration d'un délai de deux ans apparaît dans ces conditions d'un effet assez illusoire...)

En deuxième lieu c'est une société spécialisée dans la promotion et la gestion immobilière, dénommée SERGIC, qui a fait l'objet d'une condamnation en date du 28 mai 2019, sur plainte initiale d'un utilisateur de son site de location en ligne.

Sur les griefs formulés à l'encontre de la société SERGIC, deux fondements sont retenus par la CNIL, respectivement sur la sécurité et la confidentialité des données d'une part, et sur la durée de leur conservation d'autre part :
- concernant la sécurité et la confidentialité, la modification d'un seul caractère dans l'adresse URL du site permettait en effet à un utilisateur d'accéder aux pièces justificatives d'autres candidats à la location ; une telle absence de mise en place de procédure d'authentification, relevant pourtant « d'une précaution d'usage essentielle » selon la CNIL, a été considérée comme étant d'autant plus grave en l'espèce que les données ainsi accessibles étaient « susceptibles de révéler certains aspects parmi les plus intimes de la vie des personnes, comme les jugements de divorce » ;
- concernant la conservation des données pour une durée proportionnée, après avoir rappelé que celle-ci doit être déterminée en fonction de la finalité poursuivie par le traitement, la CNIL estime que la société SERGIC a manqué à cette obligation en conservant « *les données à caractère personnel des candidats n'ayant pas accédé à la location, pour une durée excédant dans des proportions importantes celle nécessaire à la réalisation de la finalité du traitement* ».

Tenant notamment compte de l'insuffisance de réactivité de la société SERGIC à réception du signalement de vulnérabilité, laquelle n'a été résolue qu'après un délai de six mois, la CNIL prononce une amende de 400.000 €, étant observé que ce montant représente quasiment 1 % du chiffre d'affaires annuel de cette société (exactement 0,93%, ce qui demeure en toute hypothèse assez amplement en deçà du plafond des 4 %, et a fortiori du plafond complémentaire de 20 millions d'euros) ; une « publicité » est également prévue sur les sites de la CNIL et de Légifrance.

En troisième lieu, et dans des circonstances assez similaires à l'affaire SERGIC, une société ACTIV ASSURANCES a fait l'objet d'une nouvelle condamnation en date du 18 juillet 2019, également sur information d'un utilisateur de son site Internet, permettant de demander des devis ou souscrire des contrats d'assurance automobile.

Outre un défaut de sécurité lié à l'adresse URL ayant entraîné la violation de données à caractère personnel, la CNIL a relevé, en l'espèce, une « absence de robustesse des mots de passe d'accès au compte client de la société » ; la faille était en effet sur ce site d'autant plus évidente que la simple date de naissance des utilisateurs valait mot de passe, étant ajouté que le formulaire de connexion sollicitait expressément ce format d'une part, et que cette information était par ailleurs adressée aux clients par courriel non crypté d'autre part.

Pour fixer le montant de la sanction, tout en précisant avoir tenu compte de la célérité de la réaction de la société ACTIV ASSURANCES qui a remédié aux défauts de sécurité dans les 24h de leur signalement, la CNIL prononce une amende de 180.000 € à son encontre (soit 1,68 % du chiffre d'affaires) ; la sanction complémentaire de publicité sur les sites de la CNIL et de Légifrance est encore prononcée, s'avérant donc pour l'instant systématique.

En synthèse sur ces trois premières décisions appliquant la nouvelle réglementation RGPD, la CNIL apparaît concentrer son contrôle :
- en amont sur le droit des usagers au moment de la collecte de données dont ils doivent être clairement informés afin de donner leur consentement de manière éclairée,
- en aval sur les failles de sécurité, a fortiori lorsqu'elles sont signalées par les utilisateurs concernés - ces trois condamnations ayant été prononcées sur plainte.

***

Après une première année 2018 placée sous le signe de la pédagogie, la CNIL a officiellement annoncé en 2019, notamment aux termes d'un communiqué du 23 mai, qu'elle vérifierait désormais « pleinement le respect des nouvelles exigences » dans l'instruction des plaintes et dans ses contrôles, et qu'elle en tirerait « au besoin toutes les conséquences, y compris en termes de sanction » : ces trois premières décisions en témoignent effectivement, et invitent les responsables de traitement à d'autant plus de vigilance - juridique comme informatique - pour éviter de telles difficultés.

Julie GRINGORE
DERBY Avocats
Réseau SIMON

Derby AVOCATS

n°73
[Octobre - Novembre 2019]

www.village-justice.com

Le Journal du Management
juridique et réglementaire

legi team Editions