AVOCATS EN DROIT DES AFFAIRES

LES SANCTIONS SOUS LE RGPD

Le RGPD a non seulement renforcé les obligations en matière de traitements de données à caractère personnel, mais a surtout assorti les manquements à ces obligations de sanctions pécuniaires qui peuvent être lourdes pour les entreprises (1). Toutefois, il convient de rappeler que des garde-fous existent et que la CNIL devra nécessairement prendre en compte certains principes essentiels tels que la proportionnalité ou la personnalité des peines (2).

1) LES AMENDES

a) Des montants dissuasifs

Le règlement donne aux autorités de contrôle la possibilité de prononcer des amendes administratives pouvant atteindre, selon la catégorie de l'infraction :

- 10 millions d'euros ou 2% du CA annuel mondial (montant plus élevé retenu)
- 20 millions d'euros ou 4% du CA annuel mondial (montant plus élevé retenu)

Cette augmentation est bienvenue puisque, jusqu'à présent, les pouvoirs de la CNIL semblaient parfois insuffisants et peu dissuasifs[1].

On rappellera toutefois que ces montants sont des plafonds.

En synthèse, le premier plafond vise plutôt à sanctionner une entreprise qui n'aurait pas mis en place les mesures technique, organisationnelles et logistiques nécessaires, tandis que le second plafond vise à sanctionner un non-respect des droits accordés aux personnes dont les données sont traitées ainsi que des transferts hors-UE réalisés en violation des règles prescrites par le règlement.

Le tableau ci-dessous donne quelques exemples des manquements pouvant entraîner l'application de l'un ou de l'autre de ces montants.

10 millions d'euros ou 2% du CA annuel mondial	**20 millions d'euros ou 4% du CA annuel mondial**
Absence de mesures effectives permettant une protection des données dès la conception et par défaut (minimisation des données collectées, durée de conservation limitée…) (article 25)	Traitement ne respectant pas les « principes de base » (par exemple : sans consentement de la personne concernée alors qu'il était requis) (articles 5, 6, 7 et 9)
Mesures de sécurité insuffisantes (article 32), recours à un sous-traitant qui ne présenterait pas les garanties suffisantes, absence de clause dans le contrat RT/ST prévoyant les obligations du sous-traitant (article 28)	Non-respect des droits des personnes (information, droit d'accès, droit de rectification, droit à l'affinement, droit à la portabilité…) (articles 12 à 22)
Non tenue d'un registre des activités de traitement (article 30), Non réalisation d'une analyse d'impact dans les cas où elle serait requise (article 35), Non désignation d'un DPD s'il est requis (article 37)	Transfert de données hors UE réalisé en violation des dispositions encadrant ce transfert (articles 44 à 49)
Absence de notification à l'autorité de contrôle et à la personne concernée en cas de violation de DCP (ou tardive) (articles 33 et 34)	Non-respect d'une injonction ordonnée par une autorité de contrôle (article 58)

[1] On se souviendra des amendes de 150.000 euros infligées par la CNIL à Google (Délibération n°2013-420 du 3 janvier 2014) puis à Facebook (Délibération n°SAN – 2017-006 du 27 avril 2017). La Loi Informatique et Libertés plafonnait en effet le montant des amendes à 150.000 euros, voire 300.000 euros en cas de récidive. La loi n°2016-1321 du 7 octobre 2016 (loi pour une République numérique) a récemment augmenté ce plafond à 3 millions d'euros. (voir article 47 de la Loi Informatique et Libertés).

MARCEAU AVOCATS
71, avenue Marceau – 75116 Paris
Tel: +33 (0) 1 53 57 90 10
Fax: +33 (0) 1 40 70 09 65
http://www.marceau-avocats.com

On précisera à titre informatif que les amendes ne sont pas déductibles des bénéfices soumis à l'impôt [2].

b) Même pour les sous-traitants !

Un des apports majeurs du RGPD est d'avoir considérablement élargi les obligations du sous-traitant en les assortissant des mêmes amendes administratives que celles prévues pour le RT[3].

C'est un réel changement.

En effet aujourd'hui, les obligations du sous-traitant dans la Loi Informatique et Libertés se limitent à assurer la sécurité du traitement et la confidentialité des données[4] et ces obligations ne sont assorties d'aucune sanction.

Ainsi et encore récemment, la société HERTZ a été condamnée au paiement d'une amende de 40.000 euros pour une faille de sécurité causée par une erreur de son sous-traitant en charge du développement du site internet[5].

Demain avec le RGPD, cette situation sera rééquilibrée :

- Nombreuses des obligations imposées au RT s'imposeront aussi au ST (exemples : désigner un DPD, tenir un registre des traitements, mettre en place les mesures de sécurité appropriées, notifier une violation de DCP)
- Par ailleurs, le RGPD prévoit expressément que le ST pourra être contrôlé et sanctionné par l'autorité de contrôle au même titre que l'est aujourd'hui le RT.

c) Et même pour les traitements déjà existants avant l'entrée en vigueur du RGPD ?

Les sanctions pourront-elles s'appliquer à des traitements non conformes mis en œuvre avant la date d'entrée en vigueur du RGPD ?

Si l'application effective du RGPD a été retardée de deux ans, c'est justement pour permettre (notamment) une mise en conformité des traitements déjà existants.

Le considérant 171 du RGPD précise qu'il abroge la directive 95/46/CE et que les traitements déjà en cours devraient être mis en conformité dans un délai de deux ans après son entrée en vigueur (soit avant le 25 mai 2018).

Il faut pourtant garder en vue le principe de non-rétroactivité des sanctions, qui interdit de condamner une entité pour des faits qui n'étaient pas légalement répréhensibles au moment où ils ont été commis.

La question se pose surtout pour les obligations préalables à la mise en place d'un traitement : une application stricte du principe de non-rétroactivité conduirait à estimer que ces obligations (modalités de recueil du consentement, informations des personnes, analyse d'impact préalablement à la mise en place d'un traitement à risque…) telles qu'imposées par le RGPD ne s'appliqueraient pas aux traitements existants avant le RGPD, puisque précisément elles n'existaient pas (ou pas avec la même ampleur) à l'époque.

---

[2] Article 39-2 du Code Général des Impôts : « *Les sanctions pécuniaires et pénalités de toute nature mises à la charge des contrevenants à des obligations légales ne sont pas admises en déduction des bénéfices soumis à l'impôt* ».

[3] On précisera toutefois que la notion de « sous-traitant » au sens du RGPD doit être entendue de façon large, et ne doit pas être limitée à la notion juridique française de sous-traitant. Il s'agira en fait de tout fournisseur / prestataire qui opère un traitement de données personnelles pour le compte du responsable de traitement. A ce titre, les termes de « controller » (pour responsable de traitement) et « processor » pour sous-traitant sont sans doute plus parlants.

[4] Article 35 de la Loi Informatique et Libertés

[5] délibération de la CNIL n°SAN-2017-010 du 18 juillet 2017

Il faut toutefois rester très prudents avec cette analyse. Quelques pistes ont pu être données. Le considérant 171 du RGPD précise par exemple, au sujet du consentement, que : « Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement. » Cela impliquerait donc de redemander un consentement si ce dernier n'est pas « conforme RGPD.

Quant à l'analyse d'impact, le G29 a précisé que l'obligation ne s'appliquerait qu'aux opérations de traitement initiées après l'entrée en vigueur du RGPD, bien qu'il recommande vivement d'y procéder pour les traitements antérieurs6.

Pour les obligations « post-traitement » (tenue d'un registre des activités de traitements par exemple), la réponse est plus claire : il faut se mettre en conformité avant mai 2018[7] !

d) D'autres sanctions ?

Le RGPD prévoit que les Etats Membres peuvent prévoir d'autres sanctions, « *en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83* »[8].

Par exemple en France, le Code Pénal prévoit aujourd'hui toute une série de manquements à la Loi Informatique et Libertés qui peuvent être punis de cinq ans d'emprisonnement de 300.000 euros d'amende.

Il faudra donc attendre la nouvelle Loi Informatiques et Libertés pour savoir comment la France se positionnera par rapport à ces sanctions supplémentaires.

Par ailleurs, on rappellera que, à côté des amendes pouvant être imposées par la CNIL, une société qui commet un manquement aux obligations du RGPD peut voir sa responsabilité engagée par toute personne qui a subi un dommage[9] (là où les amendes CNIL peuvent être prononcées même si aucun dommage n'a été subi).

Les victimes devront donc prouver un dommage matériel ou moral. Face à une procédure qui peut s'avérer longue, complexe et coûteuse, elles peuvent se trouver découragées. Seule une action de groupe permettrait, à notre sens, de mettre en pratique cette possibilité pour les victimes. Or aujourd'hui, en France, les actions de groupe sont restreintes et elles ne permettent pas de demander des dommages-intérêts[10].

---

[6] Par ailleurs l'analyse d'impact devra être réalisée pour un traitement antérieur si celle-ci devient nécessaire suite à une modification du contexte du traitement (exemple : décision ultérieure de transférer les données hors UE).

[7] On pourrait également penser que les exigences de « privacy by design » ne s'appliqueraient pas aux logiciels et outils déjà installés à la date d'entrée en vigueur du règlement, mais uniquement au moment de la première mise à jour / nouvelle version, à l'instar de ce qui est prévu dans le projet de règlement e-privacy en ce qui concerne les possibilités de paramétrer les préférences cookies au niveau des navigateurs.

[8] Article 84 du RGPD

9 article 82 du RGPD – On précisera que le déléguée à la protection des données (DPD) n'est pas responsable en cas de manquement du responsable de traitement à ses obligations issues du RGPD. Seul le responsable de traitement ou le sous-traitant répondra des éventuels manquements aux dispositions légales en vigueur.

10 L'action de groupe, introduite par la loi du 18 novembre 2016 de modernisation de la justice du XXIe siècle, est ouverte lorsque plusieurs personnes physiques subissent un dommage ayant pour cause commune un manquement à des dispositions légales, parmi lesquelles la loi du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle permet d'obtenir la cessation du manquement mais non la réparation des préjudices subis. Elles ne sont ouvertes qu'aux associations de défense des consommateurs / de protection de la vie privée et des données personnelles ainsi qu'aux organisations syndicales.

L'action de groupe pourrait, à moyen terme, voir son périmètre étendu à la réparation des préjudices subis. Dans cette hypothèse, les entreprises devraient être d'autant plus vigilantes puisqu'elles pourraient être exposées, en cas de dommages, à des demandes indemnitaires très élevées.

2) LES GARDEFOUS

Les montants des sanctions édictés par le RGPD a suscité de vives inquiétudes.

Toutefois, il convient de rappeler quelques principes qui permettront de rassurer les entités soumises au RGPD.

a) Une démarche progressive

La CNIL a souhaité rappeler que la mise en conformité et le principe de « responsabilisation » doit être élaborée en collaboration avec les régulateurs. Elle se positionne ainsi, au début du moins, plus comme un accompagnateur que comme un organe de sanction

Elle a rappelé qu'il ne fallait pas voir le RGPD comme un « couperet » en 2018. « *Il faut déconstruire cette idée qu'il y aura un coup de tonnerre en mai 2018 et que, comme des petits soldats, il faut que les entreprises soient prêtes à 100 %* »[11].

Aussi, en mai 2018, la CNIL attendra des entreprises qu'elles puissent prouver qu'elles ont largement enclenché la mise en conformité et qu'elles ont les « réflexes RGPD », et non pas qu'elles soient 100% compatibles, ce qui ne serait pas raisonnable.

b) Le principe de proportionnalité [12].

Ce principe implique qu'une sanction soit adaptée à la gravité du manquement reproché. Il s'impose non seulement à l'auteur du texte édictant une sanction, mais aussi à l'autorité qui inflige la sanction.

En France, il a valeur constitutionnelle.

Ce principe apparaît d'ailleurs en filigrane dans le texte du RGPD, qui précise que, pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende, il devra être tenu compte de plusieurs critères tels que :

- la nature, la gravité et la durée de la violation (finalité du traitement, nombre de personnes affectées, niveau du dommage),
- le fait que la violation ait été commise délibérément ou par négligence :
- les mesures prises pour atténuer le dommage
- les catégories de données concernées
- etc…[13]

On rappellera que les autorités de contrôle se voient conférer, à côté du pouvoir de prononcer des amendes lourdes, d'un arsenal de dispositifs pour permettre le respect des principes RGPD.

[11] Isabelle Falque-Pierrotin, présidente de la CNIL, https://www.contexte.com/article/numerique/rgpd-cnil-falque-pierrotin_71510.html

[12] érigé en « principe général du droit » par la CJUE (CJCE, 17 décembre 1970, *Internationale Handelsgesellschaft*, aff. 11/70) puis consacré par l'article 5§4 du traité sur l'Union Européenne. Edicté à l'article 8 de la Déclaration Universelle des Droits de l'Homme de 1789 : « la loi ne doit établir que des peines strictement et évidemment nécessaires ».

[13] Voir article 83§1 du RGPD

Cela peut aller d'un simple avertissement (rappel à l'ordre) à des injonctions de faire et des interdictions. La CNIL pourra interdire un traitement, ordonner la suspension des flux de données qui partiraient vers un pays hors UE, ou encore retirer une certification.

L'amende n'est donc pas l'unique outil et le principe de proportionnalité impose que la CNIL en fasse un usage adapté à la gravité du manquement.

c) Le principe de personnalité

Par ailleurs, le principe de personnalité impose qu'une personne ou une entreprise ne puisse pas être condamnée en raison du manquement ou d'une infraction commise par une autre personne.

Cela signifie pas toutefois qu'un responsable de traitement ne puisse pas être condamné en raison d'une défaillance de son sous-traitant : en effet, un responsable de traitement qui ne vérifie pas que son sous-traitant présente des garanties de sécurité suffisantes commet de ce fait-même, lui aussi, un manquement, et peut être sanctionné à ce titre.

La décision HERTZ précitée (voir note 4) en est un bon exemple : la CNIL relève que la société n'a imposé aucun cahier des charges à son sous-traitant concernant le développement du site internet, et ne s'est pas assurée que la mise en production du site internet avait été précédée d'une série de tests permettant de s'assurer de l'absence de vulnérabilité. Elle considère à ce titre que « *la violation de données résulte d'une négligence de la société [HERTZ] dans la surveillance des actions de son sous-traitant* »[14].

d) Le droit à un recours devant le Conseil d'Etat – exemple avec l'arrêt « optical Center », du 19 juin 2017

Le RGPD rappelle que « *toute personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne* ». (article 78)

En France, c'est le Conseil d'Etat qui est compétent pour examiner les recours dirigés contre les décisions et sanctions de la CNIL.

Un arrêt récent du Conseil d'Etat illustre le contrôle de proportionnalité effectué par cette juridiction. La CNIL avait constaté que la société OPTICAL CENTER n'avait pas respecté la mise en demeure qui lui avait été adressée et visant à mettre en place un dispositif sécurisé type https lors de l'accès au site web. Elle a prononcé une amende de 50.000 euros et a prévu que la publication de la décision sur le site de la CNIL et sur le site Légifrance. La société OPTICAL CENTER a effectué un recours devant le Conseil d'Etat.

Si la sanction principale (l'amende) n'a pas été jugée disproportionnée, ce n'est en revanche pas le cas de la sanction complémentaire de publication. Le Conseil d'Etat a en effet jugé que : « *En l'espèce, eu égard à la renommée et à l'importance de la société, la sanction complémentaire contestée, qui vise à renforcer le caractère dissuasif de la sanction principale en lui assurant une publicité à l'égard du public, est justifiée, dans son principe, au regard de la gravité et de la persistance des manquements constatés aux dispositions de la loi du 6 janvier 1978. Toutefois, si la délibération attaquée prévoit que cette publication est effectuée sur le site internet de la CNIL et sur le site Légifrance, elle ne précise pas la durée de son maintien en ligne sur ces deux sites. En omettant de fixer la durée pendant laquelle la*

[14] Ce contrôle du sous-traitant passe également par l'insertion de clauses contractuelles relatives à la sécurité, et le choix de sous-traitants qui adhèrent à des codes de bonne conduite ou ont obtenu des certifications (ces 2 outils « RGPD » ne sont pas encore disponibles à l'heure où cet article est rédigé).

publication de la sanction resterait accessible de manière non anonyme sur ces deux sites, (…) la formation restreinte de la CNIL doit être regardée comme ayant infligé une sanction complémentaire excessive car sans borne temporelle. Il y a lieu, dans les circonstances de l'espèce, de limiter à deux ans le maintien en ligne de la sanction non anonymisée sur les deux sites considérés. »[15]

***

Les Autorités de contrôle se sont montrées rassurantes quant à l'application qui sera faite de la règlementation au cours des premiers mois de son entrée en vigueur. Toutefois, il est important de garder à l'esprit qu'une entreprise qui ne s'est pas investie dans les démarches RGPD s'expose à des sanctions lourdes. Il est donc urgent de s'y préparer.

[15] Conseil d'État, 10ème - 9ème chambres réunies, 19/06/2017, 396050