

Protection des données personnelles : les entreprises bel et bien contraintes | Le Net Expert Informatique



Pensée pour protéger le citoyen, la loi Informatique et Libertés est de plus en plus détournée de son objectif premier. Tant par les salariés que par les entreprises elles-mêmes, qui n'hésitent plus à s'en servir comme arme concurrentielle. L'analyse de l'avocat François Coupez.

La protection des données à caractère personnel est née en France avec la loi du 6 janvier 1978 dite « Informatique et Libertés ». Le texte a été modifié en 2004 (à la suite de la directive européenne 95/46), et il est destiné à l'être à nouveau par le projet de loi sur le numérique annoncé en grande pompe depuis deux ans maintenant... avant d'être de toute façon complètement remplacé par un projet de règlement européen ([http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?l3Reference=2012/0811\(COD\)%26l1=fr](http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?l3Reference=2012/0811(COD)%26l1=fr)) encore en discussion qui unifiera en 2017 ou 2018 le droit de tous les pays de l'Union européenne sur le sujet.

Si ces différents projets visent à accroître de façon très importante les sanctions financières, ils ont également pour but de permettre une application plus efficace des règles (droit à l'oubli numérique/au déréférencement, co-responsabilité des sous-traitants, etc.). Mais en parallèle, on constate depuis quelques années le développement d'une véritable instrumentalisation de cette protection légale, aux règles extrêmement formelles et aux impacts potentiellement dévastateurs[1] sur l'image des entreprises prises en fautive.

Salariés et clients, quand le pouvoir change de camp

Historiquement, la CNIL a eu l'occasion d'appliquer les principes de la loi « Informatique et Libertés » dans plusieurs domaines, avec la plupart du temps deux points communs : d'une part la protection des clients contre l'utilisation qui serait faite de leurs données en contradiction avec les règles applicables et, d'autre part, la protection des salariés dans des hypothèses de surveillance abusive, de discrimination ou de mode d'évaluation des performances illicites.

Dans les deux cas, l'action de la CNIL conduit souvent l'entreprise fautive à revoir beaucoup plus globalement l'ensemble de ses processus et leur conformité.

Or les difficultés pratiques concernant le respect de cette réglementation pour l'entreprise ne doivent pas être sous-estimées. Elles tiennent tant à son formalisme qu'à ses conditions d'application, étant entendu que les traitements de ce type de données se développent de façon exponentielle avec la transformation numérique. De plus, l'entreprise, confrontée à un lacis réglementaire croissant et dans tous les domaines, alloue parfois ses ressources pour se mettre en conformité en fonction de l'urgence, ou du risque réel de sanction. Les entreprises ne peuvent ainsi pas toujours prétendre réussir un sans-faute en matière de protection des données personnelles, et en sont pleinement conscientes.

En parallèle, un phénomène se développe depuis quelques années, à un point tel qu'il se généralise. Sentant la faille, des clients ou des salariés bien informés n'hésitent plus à l'utiliser, non pour faire valoir leurs droits en la matière, mais pour faire pression dans le cadre d'un contentieux ou d'une revendication autre. La réglementation devient alors un simple prétexte destiné à faire plier son opposant.

Concernant le cas des clients, cela concerne souvent les entreprises disposant de nombreux points de contact avec la clientèle (et disposant de nombreux conseillers clientèles, etc.). Dans les grands réseaux, il est toujours plus difficile de faire respecter à tous les salariés en contact avec la clientèle les règles de base (notamment concernant la zone de « bloc-note » ou de note en champ libre sur les fiches clients, propices à tous les excès), ce qui multiplie les hypothèses de manquements :

Quant aux salariés, il est de plus en plus fréquent qu'ils fassent jouer leurs droits en la matière. Par exemple, l'une des pratiques les plus fréquentes est de systématiquement avoir recours au droit d'accès aux données personnelles que leur employeur collecte sur eux, lorsque le contrat de travail arrive précocement à son terme, ou que les deux parties se retrouvent aux Prud'hommes. La pratique montre ainsi que, sur l'ensemble des personnes pouvant faire valoir leur droit d'accès dans le cas de traitements réalisés par une entreprise, près de 75% des demandes proviennent de l'intérieur et donc des salariés. Ainsi, il n'y a qu'à regarder la jurisprudence en droit social ces dernières années pour s'apercevoir qu'il est devenu aussi courant d'alléguer un traitement de données personnelles contraire à la loi, et donc de l'illicéité du moyen de preuve opposé à un salarié, que d'en appeler aux pages Facebook en matière de divorce. Un exemple récent nous vient de l'arrêt de la Cour d'appel de Rouen rendu le 12 mai 2015 qui invalide les preuves concernant d'une part un système de badgeage (pas d'information du comité d'entreprise) et d'autre part un logiciel permettant de contrôler les horaires des salariés (pas de formalités CNIL) : le licenciement est ainsi considéré comme étant sans cause réelle ni sérieuse.

Maintenant les contentieux... entre entreprises ?

Ce qui est plus marquant encore, c'est que ce phénomène est en passe de gagner les relations entre entreprises.

Alors que l'on s'attend à ce que ce soit la victime (client, salarié, etc.) qui fasse valoir les droits qui lui sont reconnus, les tribunaux sont en effet saisis de façon croissante de manquements à cette réglementation allégués par... des sociétés concurrentes.

Pour mettre fin à un partenariat commercial, annuler une vente, tenter de prouver une rupture abusive des relations commerciales ou empêcher un concurrent de commercialiser un service innovant, les hypothèses se multiplient dans lesquelles des tribunaux de tout type sont confrontés à cette situation.

En voici quelques exemples :

le 25 juin 2013, la Cour de cassation a rendu une décision conduisant à l'annulation de la vente d'un fichier de clients informatisé. Dans cette affaire, les associés d'une entreprise avaient vendu pour 46 000 € le seul fichier des clients de l'entreprise, fort de 6 000 clients référencés depuis 1946. Or pour l'acheteur ayant utilisé quelques semaines cette base, celle-ci était une coquille vide de 1 950 clients actifs seulement. Il en demandait donc le remboursement, qu'il obtint : pour la Cour de cassation, l'absence du respect des formalités CNIL rend toute commercialisation du fichier impossible, la vente ayant nécessairement un objet illicite.

À la suite d'une décision de la CNIL du 8 septembre 2011 autorisant pour la première fois une entreprise à traiter pour des raisons commerciales le numéro NIR (aussi appelé « numéro de sécurité sociale »), une entreprise concurrente a formé un recours considérant que l'interprétation était contestable au sens de la loi Informatique et Libertés et qu'elle conduisait à un avantage concurrentiel injustifié. C'était le premier recours intenté à l'encontre d'une décision d'autorisation, alors qu'en général – et logiquement – les recours sont formés en cas de refus de la CNIL. Or, le Conseil d'Etat, s'il a confirmé la décision de la CNIL le 26 mai 2014, a surtout reconnu le droit à agir de la société concurrente dans cette affaire (voir, à ce sujet, l'excellent article de Guillaume Desgens-Pasanaou dans Expertises N° 391 de Décembre 2014 : « Données personnelles : ouverture de l'usage du NIR au secteur privé »).

Dans une affaire récente de rupture abusive alléguée de relations commerciales, la société se plaignant de la rupture (société B) proposait à l'autre société (A) de numériser pour elle des documents dans lesquels figuraient des données personnelles, et d'effectuer cette prestation depuis le Vietnam. La société A aurait donc dû demander l'autorisation de la CNIL du fait des flux de données vers ce pays, ce qu'elle n'a pas fait. Inaction qui, pour la société B, constitue un élément de preuve que la société A ne croyait en réalité pas au projet et ne comptait pas sérieusement contracter avec elle. La Cour d'appel de Paris toutefois, pour des raisons de défaut de preuve, n'a pas suivi cette analyse et a considéré le 10 avril 2015 qu'il n'y avait pas de rupture abusive.

Le grand classique des contentieux de demain ?

On le voit à travers ces quelques exemples jurisprudentiels récents, le phénomène va croissant. Il est surtout appelé à prendre encore de l'ampleur avec le futur projet de règlement européen, qui conduit à remplacer les formalités préalables par un contrôle constant de conformité et oblige donc à documenter la façon dont les traitements sont opérés à toutes les étapes. Or toutes ces informations forment un vivier de preuves de ce qui a été fait (ou pas), destinées au régulateur... et qui pourraient facilement être utilisées par une société concurrente dans le cadre d'un procès.

Plus globalement, les entreprises doivent prendre conscience de cette évolution et en saisir toutes les opportunités, mais également tous les risques : il semble logique que les études de risque, réalisées préalablement à la mise en œuvre de traitement de données à caractère personnel, aient également à prendre en compte cette nouvelle donne.

A terme en effet, en cas de contentieux et dès que l'on parlera de près ou de loin de données, la vérification de la licéité des traitements de données personnelles de l'entreprise adverse pourrait devenir un préalable aussi convenu que la vérification des pouvoirs du signataire d'un acte.

Si cette évolution peut paraître critiquable car compliquant encore les dossiers en justice, elle est malgré tout le signe que la réglementation sur les données personnelles s'ancre profondément dans les habitudes. Un réel progrès, et qui n'était pas chose évidente il y a encore quelques années...

[1] Certes, 17 textes pénaux prévoient une sanction de 5 ans d'emprisonnement et de 1 500 000 € d'amende pour les entreprises qui enfreindraient les règles en la matière, mais les applications jurisprudentielles sont rarissimes. Les sanctions de la CNIL sont quant à elles beaucoup plus fréquentes, avec des montants financiers pour le moment limités à 150 000 € (le double en cas de récidive), seul Google Inc. ayant été condamné à une telle peine. Leur efficacité est fortement renforcée par leur publication (fort effet d'image sur les grandes entreprises).

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.silicon.fr/protection-donnees-personnelles-loi-instrumentalisee-116895.html>

Par François Coupez, Avocat à la Cour, Associé du cabinet ATIPIC Avocat et titulaire du certificat de spécialisation en droit des nouvelles technologies