MAG SECURS

LE MAGAZINE DE LA SÉCURITÉ DE L'INFORMATION

DPO/DPD

- RGPD : DPO interne ou DPO externe ?

Reportage

- La Cyber Valley bretonne dans les starting-blocks

Attaques & Solutions

- Endpoint : un maillon faible... mais vital
- Démantèlement du botnet Retadup

Juridique

- Quand l'audit s'impose en droit du numérique

QUELLE GOUVERNANCE POUR LES DONNÉES ?

Entretien avec...

Marie-Laure Denis, Présidente de la Cnil

« La Cnil entend conserver un rôle moteur de la diplomatie de la donnée personnelle »

N°62 - 18€

PC presse

4ème trimestre 2019

Quand l'audit s'impose en droit du numérique

L'audit n'est pas inconnu du droit. En droit général, l'audit se définit comme une mission de vérification de la conformité d'une opération ou de la situation d'une entreprise aux règles de droit.

L'audit a fait une entrée en force avec le RGPD[1] et son entrée en application le 25 mai 2018. Également, on entend souvent le terme d'audit à propos de l'audit de licences de logiciels pratiqué par de grands éditeurs de logiciels sur leurs parcs utilisateurs. Pour illustrer la place de l'audit dans le droit du numérique, nous analyserons le RGPD, qui est un Règlement équivalant à une Loi, et qui a fortement recours à l'audit. Ensuite, nous balancerons les forces et les faiblesses de l'exercice du point de vue de son efficacité.

RGPD, L'AUDIT À TOUS LES ÉTAGES

Le RGPD est plein de l'audit. On le trouve d'abord à l'article 28 qui régit le statut juridique du sous-traitant.

Pour mémoire, le sous-traitant au sens du RGPD est ce professionnel qui traite des données personnelles pour le compte d'un responsable de traitement. C'est l'hébergeur qui stocke les données personnelles de ses clients ou encore l'éditeur d'un logiciel en mode SaaS qui en fait de même avec les utilisateurs de son logiciel et de ses services. Le sous-traitant agit dans le cadre d'un contrat. Les grandes lignes de ce contrat sont énoncées par le Règlement. Parmi celles-là, le RGPD impose au contrat liant le sous-traitant à son client qu'il met *« à disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues [par la Loi] et pour permettre la réalisation d'audits »*. En résumé, il s'agit de sécuriser l'entière chaîne de traitements des données personnelles. A quoi sert d'imposer des obligations à celui qui est le responsable d'un traitement, si son sous-traitant traite de ces mêmes données de manière irresponsable ? Aussi, la réalisation d'audits de contrôle par un tiers fait partie du dispositif. Mais elle entend également donner au responsable de traitement les moyens de son contrôle, c'est pourquoi le RGPD lui-même, impose l'audit prévu à cet article 28.

Le Règlement a aussi créé un Délégué à la protection des données dit DPO, véritable commissaire aux comptes des données personnelles. Or, comme le commissaire aux comptes audite les comptes de l'entreprise à laquelle il est attaché pour vérifier leur régularité, l'article 39 prévoit expressément que le DPO réalise des audits pour *« contrôler le respect du présent règlement »* et même toute la réglementation en matière de données personnelles. Le RGPD prévoit également la possibilité de mettre en place pour les groupes d'entreprises établis dans plusieurs Etats, ce que l'on nomme des « règles d'entreprises contraignantes » dites BCR[2].

1: Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

2: Binding Corporate Rules

L'auteur

Olivier ITEANU est Avocat à la Cour d'Appel de Paris depuis 1989. Chargé d'enseignement à l'Université de Paris I Sorbonne en droit du numérique, il est Fondateur et Gérant de la SELARL ITEANU AVOCATS, un Cabinet d'Avocats composé de 12 professionnels basé à Paris 8ème, 164 rue du Faubourg Saint-Honoré, dédié au droit du numérique et des communications électroniques. Il est par ailleurs Vice-Président de l'Association Cloud Confidence (aujourd'hui fusionnée avec Hexatrust) et Administrateur et Secrétaire Général d'Eurocloud France, Président d'honneur du Chapitre Français de l'Internet Society (ISOC France).

Le processus prévoit que la Cnil doit approuver ces BCR. L'article 47 du RGPD prévoit que ces BCR doivent faire l'objet *« d'audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits des personnes concernées »*. Le résultat de cet audit doit être communiqué au DPO ou celui qui en tient lieu, le Conseil d'administration de l'entreprise qui exerce le contrôle sur le Groupe d'entreprises et mis à disposition de la Cnil. Enfin, la Cnil elle-même et toutes les autorités de contrôle indépendantes de l'Union Européenne se voient reconnaître dans leurs pouvoirs par le Règlement (article 58), de *« mener des enquêtes sous la forme d'audits sur la protection des données »*. On le voit donc bien, en plus d'être partout, l'audit est un instrument essentiel de la mise en conformité des organisations soumises au RGPD.

FORCES ET FAIBLESSES DE L'AUDIT

L'audit est-il la solution, pour évaluer la conformité des organisations à une norme juridique de référence, comme le RGPD ? La réponse est difficile car elle dépend en premier lieu de celui qui est en charge de l'audit, l'auditeur.

Durant les mois qui ont précédé la mise en application du RGPD en mai 2018, on a vu fleurir quantité d'acteurs intronisés spécialistes et auditeurs du RGPD. Parfois sans méthode et sans connaissance pratique du texte, ils ont souvent compliqué les choses, plutôt que de les solutionner. Or, être auditeur ne s'improvise pas. Il existe dans ce domaine des formations et des certifications.

La première faiblesse de l'outil de contrôle d'une mise en conformité est donc la personne de l'auditeur lui-même. Mais si l'auditeur est bien choisi, et des critères objectifs de choix peuvent figurer le concernant au contrat qui prévoit l'audit de contrôle, cette faiblesse peut devenir une force. Enfin, sur ce premier point, on ne doit pas oublier que l'auditeur pourrait avoir accès à des informations confidentielles dans le cadre de sa mission. Le futur audité a donc intérêt à prévoir que l'auditeur s'obligera à un engagement de confidentialité vis-à-vis des informations dont il aura connaissance.

En second lieu, même si l'audit est prévu dans un texte valant Loi comme le RGPD, l'audit est un processus avant tout contractuel. D'ailleurs, le RGPD demande à ce que la possibilité du recours à l'audit figure au contrat liant le responsable de traitement, en d'autres termes le client, et le sous-traitant au sens du RGPD, en d'autres termes le prestataire de services. Cependant, chacun aura remarqué que les modalités de l'audit ne sont pas précisées dans le Règlement. Ces modalités restent donc de la responsabilité des co-contractants. Les questions à traiter sont notamment les suivantes ; quelle est la fréquence de l'audit : une fois par an ou plus ? L'auditeur doit-il s'annoncer préalablement par courrier au sous-traitant et respecter un préavis avant de ses présenter dans les locaux ? Y a-t-il une durée maximale à l'audit, un, deux jours, car l'audit peut perturber le fonctionnement de l'entreprise ? Qu'a-t-il le droit de faire ou de ne pas faire : par exemple, l'auditeur peut-il emporter des documents ou simplement les consulter sur place sans en prendre copie ?

Ce sont quelques-unes des questions qui ne figurent pas au RGPD et qui sont pourtant essentielles à convenir entre les parties. Le contrat devra les prévoir et y répondre, c'est de l'intérêt des deux parties.

En troisième lieu, l'audit de contrôle peut-être le prélude à un litige entre parties. Ce n'est pas un cas d'école, car si le contrôle révèle des manquements, plusieurs conséquences sont envisageables. Ces conséquences peuvent être, notamment, la rupture pour faute du contrat, si le contrat le permet. Ce peut-être également la plainte à la Cnil et le risque d'une procédure administrative. Les conclusions risquent de peser lourd dans la balance du litige. Si ces conclusions penchent défavorablement à l'encontre du prestataire contrôlé, celui-ci pourrait avoir le réflexe de contester les modalités de l'audit, son opposabilité, en un mot, sa validité. Il existe un grand intérêt, de part et d'autre, à imaginer un audit balancé, qui donne la parole à l'une et l'autre partie avant ses conclusions définitives.

Ainsi, la clause d'audit insérée au contrat, peut prévoir que l'auditeur pourra établir un rapport écrit de son contrôle. Il pourra ajouter l'obligation pour l'auditeur de communiquer un rapport provisoire au bénéficiaire de l'audit, son client, et en même temps à la personne auditée. La même clause devra prévoir que l'auditeur laissera à l'audité un certain délai pour réagir, et, pour ce qui le concerne, prendre en compte les observations de l'audité. Il s'agit dans ce cas pour l'auditeur de répondre aux observations de l'audité mais l'auditeur pourra bien sûr maintenir ses premières conclusions. Cette procédure contradictoire vise à renforcer la validité du rapport d'audit.

En conclusion, le législateur européen, comme français, a raison d'inciter les acteurs économiques à recourir à l'audit. C'est un rendez-vous entre les parties à un contrat, qui permet de faire un point, pour apaiser les tensions, de corriger des situations déficientes. Pour que l'audit soit une réussite, il reste cependant de la responsabilité des parties de l'organiser dans le contrat en toutes ses modalités.