Atelier EIFR du 23 mai 2019

L'impact du RGPD dans le secteur financier après un an d'application

Sophie Nerbonne, Directrice chargée de co-régulation économique, CNIL

Après un an d'application, le règlement général sur la protection des données (RGPD) ne tourne pas à la catastrophe annoncée, même si certains secteurs ont découvert la protection des données personnelles à cette occasion (cela en dépit de l'existence de la loi informatique et libertés de 1978).

Au cours de l'année 2018, la Commission nationale de l'informatique et des libertés (CNIL), constituée de 200 personnes, dont 44 % sont des juristes (leur nombre relatif tend à baisser), a enregistré plus de 11 000 plaintes, soit un tiers de plus que l'année précédente, ce qui s'explique notamment par le fait que les particuliers sont désormais plus enclins à exercer leurs droits. La commission a renforcé son rôle d'accompagnement, en intervenant notamment par des rappels pédagogiques dans le domaine du consentement. Quelque 310 contrôles, dont 204 sur place, ont été effectués, et ont donné lieu à onze sanctions, ce qui est très peu.

La CNIL s'emploie à appliquer le RGPD de façon cohérente. D'une part en accompagnant les professionnels dans leur transition numérique (en leur procurant de la sécurité juridique, en favorisant l'innovation, en aidant les entreprises à passer de l'échelle du correspondant informatique et libertés (CIL) à celle du délégué à la protection des données (DPO), en passant des labels aux certifications, ou encore en publiant des guides, des vidéos ou encore des MOOC. D'autre part en prenant en compte la cohérence géographique, par exemple dans la gestion des plaintes, dont 20 % sont désormais transnationales, mais aussi dans les domaines des contrôles et des sanctions.

La commission souhaite par ailleurs faciliter la transition numérique, en partant des besoins des utilisateurs et en utilisant la soft regulation, cela dans un esprit de confiance. C'est par exemple le cas avec les packs de conformité, réalisés en concertation avec les branches ou secteurs d'activité. Cette approche nécessite d'identifier des publics ciblés et de travailler avec des têtes de réseaux, ce qui assure un effet démultiplicateur.

La CNIL entend désormais amplifier ses actions d'accompagnement, mais aussi faire preuve d'une plus grande fermeté dans le domaine des sanctions selon trois axes : respect des droits des personnes, traitement des données des mineurs, répartition des responsabilités entre responsable du traitement des données et sous-traitant. Jusqu'ici, la sanction la plus importante, 50 millions d'euros, a été infligée à Google.

Dans le secteur financier, plus de 1000 DPO ont été désignés (à fin mai 2019) : 459 dans l'assurance, 550 dans les établissements financiers. Ces secteurs se sont bien appropriés le RGPD, c'est-à-dire en allant au-delà de la stricte conformité au texte.

Merav Griguer, Avocat Associée, Bird & Bird

Sept points doivent faire l'objet d'une attention particulière pour ce qui est de la conformité.

La remédiation et la négociation des contrats, qui sont très nombreux, y compris d'entreprise à entreprise. Il convient de se demander quelle est la qualification des parties - responsable du traitement ou sous-traitant -, car en cas de mauvaise qualification, les obligations des parties sont inadaptées et il existe un risque de sanction de la part de la CNIL (qui n'est pas liée par la qualification des parties). Les clauses sensibles lors de la négociation d'un contrat sont les suivantes : sécurité et confidentialité des données, clause d'audit, clause de coopération, clause de sous-traitance ultérieure, clause de plafonnement des responsabilités. Il est important de s'assurer que l'on dispose des moyens opérationnels de respecter ces clauses.

Les études d'impact sur la vie privée (privacy impact assessement ou PIA en anglais). Elles sont obligatoires s'agissant de certains traitements de données et l'on se reportera à la CNIL, qui publie une liste des traitements obligatoirement soumis à une analyse d'impact. Ces analyses sont également obligatoires quand deux des critères publiés dans les lignes directrices du G29 (désormais Comité européen de la protection des données) sont réunis. Quand un seul critère est réuni, l'analyse d'impact est recommandée.

Les violations de données à caractère personnel doivent être notifiées à la CNIL, documentées, et dans certains cas, communiquées aux personnes concernées. Une notification à la CNIL sur deux serait aujourd'hui infondée, d'après le cabinet Bird & Bird.

S'agissant des contrôles de la CNIL (en ligne, sur pièces, sur place ou sur audition), il faut avoir à l'esprit que les exigences et l'expertise de l'autorité administrative ne cessent de progresser. Il est recommandé de ne pas se précipiter, de ne pas vouloir répondre tout de suite à toutes les demandes, même si l'on est soumis à un devoir de collaboration.

L'entreprise doit permettre au délégué à la protection des données (data protection officer ou DPO en anglais), dont le triple rôle consiste à conseiller, à contrôler et à piloter, d'exercer ses missions.

L'accountability, soit l'obligation de mettre en œuvre des mécanismes et des procédures permettant de montrer le respect des règles, est perpétuelle : il faut sans cesse remettre à jour les documents et procédures et s'assurer de l'efficacité du dispositif.

Enfin, il convient de sensibiliser et de former les salariés afin que se diffuse une culture de la protection des données. Un outil efficace consiste en des ateliers organisés fonction par fonction.

Florence Bonnet, Directeur, TNP

Les entreprises sont confrontées à des difficultés d'ordre opérationnel quand il s'agit de mettre en œuvre le RGPD.

Dans l'organisation générale du projet, notamment quand il n'y a pas de soutien au plus haut niveau (disposer d'un budget se révèle insuffisant). Pour que se diffuse en profondeur une culture des données

personnelles, il faut réunir de nombreuses conditions : un chef de projet, des interlocuteurs capables de dialoguer avec le DPO, des compétences juridiques mais aussi techniques, une sensibilisation régulière sur les enjeux, des indicateurs de suivi, etc.

La mise en œuvre du RGPD intervient dans un contexte réglementaire déjà très chargé et chronophage.

Les entreprises n'ont pas toujours une connaissance précise de leurs applicatifs et des données traitées, a fortiori quand elles viennent de procéder à une ou des acquisitions ou quand leur architecture informatique est décentralisée.

Peu d'entreprises disposent, à ce stade, d'outils permettant soit d'inventorier l'ensemble des traitements des données, soit d'améliorer l'efficacité du processus de protection des données. Le cabinet de conseil TNP a publié un benchmark des logiciels (une cinquantaine) disponibles sur le marché, sachant qu'il n'existe pas d'outil miracle assurant l'ensemble des tâches, mais des logiciels pouvant travailler ensemble.

L'offre de logiciels est inflationniste depuis trois ans. Cependant, on voit très peu d'acteurs nouveaux proposant des solutions pleinement satisfaisantes, et il faut s'attendre à ce que tous les éditeurs du marché ne survivent pas à cette première vague.

Dominique Dupont, Directeur Risques Opérationnels et Data Protection Groupe, La Française AM

Les données personnelles touchent de nombreux domaines à La Française et se trouvent à la croisée des relations avec les clients, les locataires, les fournisseurs ou encore les dépositaires. Il s'agit donc d'un véritable actif qui constitue un enjeu stratégique pour l'entreprise. C'est un des piliers de la confiance que portent les clients à la société de gestion et s'inscrit logiquement dans l'approche ESG adoptée par le groupe. Le RGPD ne constitue cependant pas un big bang dans la mesure où le secteur de la gestion d'actifs est accoutumé à une forte pression réglementaire, notamment en ce qui concerne les relations avec les particuliers (Pripps, Mif, lutte contre le blanchiment d'argent...).

Pour relever les défis du RGPD, la société de gestion a mis en place un comité de pilotage pluridisciplinaire, a entrepris de sensibiliser les collaborateurs (publication d'une charte, e-learning, animation des équipes opérationnelles...), a nommé un délégué à la protection des données issu de la filière « risques » (ce DPO est en relations avec des correspondants dans les métiers), s'est attachée à ce que soit établie une coordination étroite entre le DPO et le responsable de la sécurité des systèmes informatiques (il s'agit d'un point essentiel) et a établi une liste d'actions prioritaires selon une approche par les risques : organiser l'accountability, ce qui a nécessité de trouver un outil de suivi, informer les clients et salariés de leurs droits, revoir les contrats, organiser les relations avec des prestataires situés en dehors de l'Union européenne, appliquer le privacy by design...

L'ensemble représente un chantier très important à l'échelle du groupe, et dont certains aspects, la revue des contrats en particulier, avaient été sous-estimés. Ce chantier s'est organisé autour de cinq thèmes : identifier et auditer les traitements, identifier clairement le rôle des acteurs, privacy by default, culture de la donnée personnelle et coordination entre DPO et RSSI.

Lucas Naja, Data Protection Officer, Groupe Arkea

Arkéa, un groupe bancaire qui dispose de 10 500 salariés, 4,5 millions de clients et de trente filiales, a mis en place une équipe dédiée à la protection des données personnelles en mars 2018 : un délégué à la protection des données « mutualisé » pour l'ensemble du groupe entouré de quatre collaborateurs, au centre d'un réseau de trente-quatre référents dans les filiales. Au total, cela représente plus de dix personnes à temps plein. Cette équipe a avant tout pour mission de « servir les métiers ». A signaler : la lettre de mission du DPO a été signée par le directeur général et le DPO est directement rattaché au directeur général.

Ce qui a été fait jusqu'ici (juin 2019) : mise en conformité, mise en place de l'organisation (dont la nomination du DPO), définition d'un cadre de référence de la protection des données.

Les chantiers en cours : choix d'un outil, principalement pour que le DPO puisse disposer d'une vision globale, définition de plans d'actions pour chaque entité, archivage et purge des données (il s'agit d'un chantier à trois ans), achèvement du corps de procédures, revue de la politique des cookies, mise à jour du cadre de référence.

Martina Duchonova, Groupe Data Privacy Officer, CNP Assurances

A CNP Assurances, qui réalise un chiffre d'affaires de 34 milliards d'euros et sert 35 millions d'assurés, le délégué à la protection des données (DPO) groupe est rattaché à la direction de la conformité. Entouré d'un adjoint et d'une équipe pluridisciplinaire de trois autres personnes, il est aussi DPO de certaines filiales et se situe au centre d'un réseau constitué de relais informatique et libertés et de DPO de filiales ou de succursales.

A noter : le RGPD est appliqué dans toutes les filiales internationales du groupe.

Par rapport à ce qui se faisait avant le RGDP en matière de protection des données, la compagnie d'assurance a d'emblée particulièrement mis l'accent sur la mise en œuvre des principes de privacy by design (nouvelles procédures de validation des projets...) et d'accountability (création d'un outil pour les analyses d'impact et d'un registre de traitement...).

La sensibilisation des salariés au thème de la protection des données personnelles, qui prend à CNP Assurances de multiples formes, a débuté il y a une dizaine d'années. Avant 2016, des informations étaient communiquées sur le risque de non-conformité (dès 2000), le site intranet comportait un volet dédié, un quizz était à la disposition des collaborateurs et la sensibilisation s'étendait aux comités directeurs des unités opérationnelles.

En 2017, le dispositif a été notamment renforcé par des actions de formation et par la construction d'un MOOC sur les fondamentaux du règlement européen. La sensibilisation s'est poursuivie en 2018 et 2019, par exemple avec une formation dispensée à tous les membres du comex et du conseil d'administration.

L'équipe « RGPD » de la compagnie d'assurance estime de première importance que soit entreprise une sensibilisation globale : cela augmente la culture générale et ancre les bons réflexes ; cela procure un avantage concurrentiel ; c'est indispensable si l'on veut être en mesure de respecter l'obligation du privacy by design ; enfin, c'est utile aussi dans la vie privée des salariés.