Publié le 28 mai 2019

Soulier Bunch, Cabinet d'avocats d'affaires basé à Paris et Lyon

Lire cet article en ligne

Contrôles et sanctions : quels enseignements tirer de l'activité de la CNIL ?

Le 15 avril dernier, la CNIL a présenté son rapport d'activité 2018, soit le bilan qu'elle tire de son activité au cours de l'année 2018 marquée par l'application du Règlement général sur la protection des données et la nouvelle loi Informatique et Libertés.

Le bilan de la CNIL et les décisions qu'elle a prises en 2018 sont autant d'expériences dont nous pouvons tirer des leçons pour prévenir les risques encourus lorsqu'on traite des données à caractère personnel.

Enseignement n°1

Près d'un contrôle sur quatre est provoqué par une plainte ou un signalement. La CNIL a reçu un nombre record de 11 077 plaintes en 2018 (Elle explique cette hausse de 32% en un an par l'effet médiatique du RGPD et une plus grande sensibilité des citoyens aux questions de protection des données), dont 73% portaient sur le non-respect de l'exercice d'un droit.

Le responsable de traitement a en effet une obligation d'information et de transparence à l'égard des personnes dont il traite les données, et celle de répondre dans les meilleurs délais aux demandes de ces personnes (de consultation, de rectification ou de suppression de leurs données).

Concrètement, à chaque fois qu'il collecte des données personnelles, le responsable de traitement doit mentionner dans le support utilisé (formulaire, questionnaire, contrat, *etc*.) un certain nombre d'informations

sur le traitement de données et donner les moyens d'exercer effectivement les droits d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement. Le plus souvent il s'agira de prévoir un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée ou la possibilité d'exercer les droits à partir d'un compte. Bien sûr, il faut mettre en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts.

Si l'on ajoute à ces chiffres la décision prise par la CNIL d'inscrire le respect des droits des personnes dans sa stratégie de contrôle pour 2019 (le programme annuel, qui a représenté 16% des contrôles en 2018, consiste pour la CNIL à définir chaque année 3 axes sur lesquels elle décide de concentrer son action de contrôle), et sa volonté de faire de la demande d'exercice des droits un préalable à sa saisine, on ne peut que conseiller à tous les responsables de traitement de bien s'assurer qu'ils informent les personnes dont ils collectent les données et répondent aux demandes qu'ils reçoivent.

Enseignement n°2

La CNIL peut réaliser des contrôles sur place, des contrôles en ligne, des contrôles sur pièces (qui consistent à demander la communication de tout renseignement ou document utile) et des auditions (qui s'effectuent dans les locaux de la CNIL, après convocation du responsable du traitement).

En 2018, un contrôle sur trois a été réalisé sur place, dans les locaux du responsable de traitement.

Le décret pris pour l'application de la Loi Informatique et Libertés prévoit « *Lorsque la commission effectue un contrôle sur place, elle informe au plus tard lors de son arrivée sur place le responsable des lieux ou son représentant de l'objet des vérifications qu'elle compte entreprendre, de l'identité et de la qualité des personnes chargées du contrôle ainsi que, le cas échéant, de son droit d'opposition à la visite (…)* ».

L'article 44, III, de la Loi Informatique et Libertés prévoit que les agents « *peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, notamment sur place ou sur convocation, tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission. Ils peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve du deuxième alinéa du présent III, par le secret médical.* »

Autant dire qu'il est indispensable de mettre en place une procédure interne de gestion d'un contrôle détaillant les différentes actions à mener en pratique, afin d'éviter toute confusion lors du contrôle.

Un contrôle sur six est réalisé en ligne, à partir donc des locaux de la CNIL qui consulte, à partir d'un service de communication au public en ligne (site internet, application, produit connecté, etc.) des données accessibles en ligne ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers. La nouvelle Loi Informatique et Libertés permet désormais à la CNIL de le faire sous une identité d'emprunt.

C’est-à-dire qu’elle peut utiliser une adresse électronique autre que la sienne ainsi qu’un pseudonyme pour effectuer des contrôles sur internet ou sur une application.

Enseignement n°3

La CNIL a prononcé 11 sanctions, dont 10 amendes, dont 9 ont été rendues publiques (dont 400 000 euros pour Uber, 250 000 euros pour Bouygues, 250 000 euros pour Optical Center[1]).

Concernant ces 9 décisions, 7 concernent des dossiers ouverts suite à une plainte ou un signalement. Elles concernent toutes des atteintes à la sécurité des données personnelles. Elles montrent que la CNIL vérifie la bonne application des règles de cybersécurité, au-delà du respect des règles « juridiques » du RGPD.

A noter que ces amendes concernent des faits qui se sont déroulés avant l’entrée en application du RGPD. Elles ont donc été prononcées sur le fondement de « l’ancienne » Loi Informatique et Libertés qui prévoyait un plafond maximal de 3 millions d’euros. Aujourd’hui, en fonction des manquements, le montant des sanctions pécuniaires en application du RGPD peut s’élever jusqu’à 20 millions d’euros ou dans le cas d’une entreprise jusqu’à 4 % du chiffre d’affaires annuel mondial.

On n’oublie pas que c’est la CNIL qui a infligé à Google, en janvier 2019, l’amende la plus importante sur le fondement du RGPD (50 millions d’euros).[2]

Enseignement n°4

La CNIL s’étend peu sur les recours introduits contre ses décisions devant le Conseil d’Etat. Il faut dire que le Conseil d’Etat a rarement l’occasion de se prononcer sur les décisions rendues par la CNIL.

Le RGPD obéissant à une logique plus répressive, il sera intéressant de suivre l’évolution de la pratique de la CNIL et d’observer – peut-être – la construction progressive d’un droit jurisprudentiel encadrant les activités de contrôle et de sanction de la CNIL.

On ne peut manquer ici l’occasion de mentionner l’arrêt rendu par le Conseil d’Etat le 17 avril 2019 par lequel il a confirmé mais réduit l’amende de 250 000 euros prononcée par la CNIL à l’encontre d’Optical Center.

Selon le Conseil d’Etat, une sanction pécuniaire prononcée par la CNIL doit notamment tenir compte du comportement du responsable de traitement suite au constat du manquement de ses obligations. En ne tenant pas compte de la célérité avec laquelle la société Optical Center a remédié aux manquements qui lui ont été reprochés, le Conseil d’Etat a considéré que la sanction infligée par la CNIL avait un caractère disproportionné et en a donc réduit le montant à 200 000 euros (soit une réduction de 20%).

[1]Cf. article intitulé Fuite de données : la CNIL impose une nouvelle amende record à Optical Center

[2]Cf. article intitulé Données personnelles : une première amende pour Google

Soulier Bunch est un cabinet d'avocats pluridisciplinaire proposant aux différents acteurs du monde industriel, économique et financier une offre de services juridiques complète et intégrée.

Nous assistons nos clients français et étrangers sur l'ensemble des questions juridiques et fiscales susceptibles de se poser à eux tant dans le cadre de leurs activités quotidiennes qu'à l'occasion d'opérations exceptionnelles et de décisions stratégiques.

Chacun de nos clients bénéficie d'un service personnalisé adapté à ses besoins, quels que soient sa taille, sa nationalité et son secteur d'activité.

Pour plus d'informations, visitez soulierbunch.com.