DERRIENNIC ASSOCIÉS

Conformité RGPD

Rapport d'activité 2019 de la CNIL

#NewsDerriennicRGPD 24

Madame, Monsieur,

Nous vous proposons, en ce mois de juillet 2020, de découvrir un numéro spécial de notre lettre d'actualité dédié au rapport d'activité 2019 de la CNIL.

Ce numéro propose un focus sur les sujets suivants :

- Les contrôles
- Les mises en demeure et sanctions
- Le plan d'action « cookies »
- La reconnaissance faciale
- La question de la sécurité

Nous vous en souhaitons une bonne lecture.

Rapport d'activité 2019 de la CNIL : les contrôles

La CNIL a rendu public, le 9 juin 2020, son quarantième rapport d'activité, dans lequel elle revient sur les opérations de contrôle qu'elle a réalisées au cours de l'année 2019.

La CNIL indique avoir procédé, durant l'année 2019, à 300 contrôles, dont :

- 169 contrôles sur place ;
- 53 contrôles en ligne ;
- 45 contrôles sur pièce ;
- 18 auditions.

Ces contrôles, en baisse par rapport à l'année 2018 (310) :

- se sont inscrits dans le cadre de l'instruction de plaintes ou de signalement (43%),
- ont été effectués à l'initiative de la CNIL, notamment au vue de l'actualité (31%) ou ont résulté des thématiques prioritaires annuelles décidées par la CNIL (21%)
- ont été réalisés dans le cadre des suites de mises en demeure ou de procédure de sanction (5%).

La CNIL précise avoir relevé, au cours de ces contrôles, des mauvaises pratiques récurrentes, telles que :

- des délais de réponses excessifs aux demandes d'exercice de droits ;
- l'absence de lien de désabonnement dans les courriels de prospection commerciale ;
- l'absence de possibilité, pour les clients, de supprimer eux-mêmes leur compte en ligne.

Lien vers le rapport annuel de la CNIL :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf

Rapport d'activité 2019 de la CNIL : focus sur les mises en demeure et sanctions

L'analyse du 40eme rapport annuel de la CNIL nous apporte plusieurs enseignements sur la politique répressive qui a été menée par la CNIL en 2019.

I) Les mises en demeure

La Présidente de la CNIL a prononcé **42 mises en demeure** dont **2 rendues publiques** qui font suite :

- Pour 52% à l'instruction de plaintes (19% en 2018) ;
- Pour 17% à la réalisation de contrôles sur le fondement de plaintes (19 % en 2018) ;
- Pour 31% à des missions effectuées sur la base du programme annuel des contrôles défini par la CNIL, ou effectuées à l'initiative de la CNIL en lien avec l'actualité (60 % en 2018).

Aucune mise en demeure n'a eu pour source une notification de violation de données à caractère personnel (le rapport d'activité 2018 recensait 2% de mises en demeures faisant suite à une notification de violation de données).

La CNIL a donc prononcé un peu moins de mises en demeures qu'en 2018, année qui avait été marquée par l'augmentation substantielle du nombre de mises en demeure rendues publiques : 49 mises en demeure dont 13 rendues publiques.

Sur la source des mises en demeures, la CNIL indique, dans son dernier rapport d'activité, que : *« L'année 2019 montre une tendance inversée par rapport à 2018 s'agissant de l'origine des mises en demeure puisque celles-ci ont dorénavant comme source principale les plaintes que reçoit la CNIL. ».*

II) Les sanctions

La formation restreinte de la CNIL a prononcé, en 2019, **8 sanctions** :

- **7 amendes administratives** dont 4 ont fait l'objet d'injonctions sous astreinte allant de 200 à 3 000 euros par jour de retard et 5 ont été rendues publiques ;
- **1 injonction sous astreinte**.

Il y a donc eu moins de sanctions prononcées en 2019 qu'en 2018 (10 sanctions pécuniaires dont 9 rendues publiques et 1 avertissement non-public).

Le montant total annuel des sanctions prononcées en 2019 s'élève à **51 370 000 euros** contre **1 196 000 euros** en 2018. Ce montant est à relativiser compte tenu de la sanction record de 50 000 000 euros prononcée à l'encontre de la société GOOGLE en janvier 2019.

Il convient de relever que la formation restreinte a fait usage, à plusieurs reprises, de son nouveau pouvoir tel que prévu par le RGPD : **l'injonction avec astreinte**.

Dans son rapport, la CNIL explique ses prérogatives dans les termes suivants :

« La formation restreinte peut, lorsqu'un responsable de traitement ou un sous-traitant ne respecte pas le RGPD ou la loi Informatique et Libertés, prononcer une injonction de mettre en conformité le traitement ou de satisfaire aux demandes d'exercice des droits des personnes. Cette injonction peut être assortie d'une astreinte, sauf dans les cas où le traitement est mis en œuvre par l'État. Son montant ne peut excéder 100 000 euros par jour de retard à compter de la date fixée par la formation restreinte. L'injonction est utilisée lorsqu'un manquement est constitué mais que le

responsable de traitement ou le sous-traitant ne s'est pas mis en conformité au jour où la formation restreinte se prononce. Cette mesure correctrice permet ainsi d'atteindre la mise en conformité dans un délai contraint puisqu'une fois ce délai dépassé, une astreinte commence à courir jusqu'à ce que le responsable de traitement ou le sous-traitant se soit mis en conformité.»

Enfin, sur les manquements relevés, nous notons que 6 sanctions sur 8 ont été prises à raison d'un manquement à **l'obligation de sécurité**.

Rapport d'activité 2019 de la CNIL : retour sur le plan d'action «cookies»

Dans son rapport d'activité 2019, la CNIL consacre un chapitre à ses actions menées en matière de cookies.

I) Le cadre juridique

La CNIL rappelle être en charge de l'application du cadre juridique français et européen en matière de cookies, qui se compose de :

- **la Directive ePrivacy** adoptée en 2002 (et révisée en 2009), qui vise à compléter et préciser le cadre général applicable au traitement des données personnelles.
- **la loi « Informatique et libertés »** qui transpose en droit français la directive ePrivacy.

II) Les enjeux

La révision de la directive ePrivacy, sous forme de règlement, a été initiée en 2017 pour assurer la bonne articulation avec le RGPD. Toutefois, la date d'adoption de ce nouveau texte étant toujours incertaine et face à la nécessité de clarifier certaines pratiques non respectueuses des droits des personnes, la CNIL a décidé en 2019 « *de faire du ciblage publicitaire une priorité* ».

L'autorité relève en effet :

- Des enjeux de protection des données très forts pour les personnes par le caractère massif et parfois très intrusif du ciblage publicitaire ;
- Un renforcement des exigences en ce qui concerne les modalités de recueil du consentement, consécutif à l'entrée en vigueur du RGPD ;
- Un grand nombre de plaintes visant le ciblage publicitaire au moyen de cookies et soulevant l'absence de recueil d'un consentement valable ;
- Un souhait des acteurs du secteur de mieux comprendre leurs obligations.

III) Plan d'action de la CNIL

Afin de faire appliquer les règles en France, la CNIL a publié en 2019 **des lignes directrices sur les cookies et autres traceurs** (ayant fait l'objet d'une décision du Conseil d'Etat), puis adopté un **projet de recommandation**.

La CNIL a souhaité aussi **développer des outils de sensibilisation** des citoyens (CookieViz) et **d'aide à la mise en conformité** pour les organismes (outil PIA, Guide du développeur…).

Sur sa **politique répressive**, la CNIL précise que :

- Les investigations initiées en 2019 sur la base des plaintes reçues se poursuivent en 2020. Celles-ci visent *« le respect des principes en vigueur depuis la révision de la directive ePrivacy intervenue en 2009, inchangés avec le RGPD, notamment le caractère préalable du consentement au dépôt de traceurs, l'information adéquate de l'utilisateur, ou encore la possibilité pour celui-ci de retirer effectivement son consentement. ».*
- Une fois la recommandation adoptée (date non-encore définie) et le délai de 6 mois accordé pour se mettre en conformité passé, la CNIL *« vérifiera alors le respect plein et entier des obligations de la loi Informatique et Libertés, y compris des nouveautés résultant de l'entrée en application du RGPD, en matière de traceurs et cookies, telles qu'éclairées par cette recommandation. »*

Sur l'argument parfois avancé selon lequel la directive ePrivacy favoriserait les géants du numérique qui proposent des univers

authentifiés, la CNIL souligne que **les mêmes règles s'appliquent à tous les acteurs** sans distinction dès lors qu'ils sont établis en Europe ou que leurs utilisateurs le sont.

Elle rappelle à cet égard que : *« Le fait que l'utilisateur soit authentifié ne dispense aucunement de recueillir son consentement, dès lors que des traceurs non exemptés de consentement sont utilisés. »*. Elle ajoute également que : *« le fait d'utiliser un seul traceur pour de multiples finalités n'exonère pas non plus de recueillir le consentement pour les finalités qui le nécessitent.*

Enfin, la CNIL précise échanger régulièrement avec ses homologues européens afin de favoriser une harmonisation des positions dès lors que **la directive ePrivacy fait l'objet d'une transposition variable d'un pays à l'autre et que son application est confiée à des autorités différentes**. Une position harmonisée ne sera réellement renforcée qu'une fois le futur règlement adopté.

Rapport d'activité 2019 de la CNIL : la reconnaissance faciale

La CNIL a rendu public, le 9 juin 2020, son quarantième rapport d'activité, dans lequel elle fournit son analyse sur un sujet sensible : la reconnaissance faciale.

La reconnaissance faciale est une « *technologie biométrique* » qui, rappelle la CNIL, « *permet de reconnaitre automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier* ».

Pour mémoire, la CNIL avait, en 2018, appelé à un débat démocratique sur ce sujet, et a contribué, en novembre 2019, audit débat, en présentant « *les éléments techniques, juridiques et éthiques qui doivent, selon elle, être pris en compte dans l'approche de cette question complexe* ».

Dans son rapport d'activité 2019, la CNIL indique que trois exigences essentielles devraient guider les réflexions sur toute expérimentation en matière de reconnaissance faciale :

- tracer des « *lignes rouges* » en faisant en sorte que la reconnaissance faciale respecte le RGPD et la directive « Police-Justice » ;
- placer le respect des personnes au cœur de la démarche, en recueillant le consentement « *pour chaque dispositif le permettant* », en gardant le contrôle des données, en assurant la transparence, en garantissant les droits de retrait du dispositif et en faisant de la sécurité des données biométriques une condition impérieuse de leur traitement ;
- adopter une démarche « *sincèrement expérimentale* », en limitant dans le temps et dans l'espace les dispositifs de reconnaissance faciale et en identifiant de façon exacte les objectifs poursuivis par les expérimentations et leurs critères de réussite.

Lien vers le rapport annuel de la CNIL :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf

Rapport d'activité 2019 de la CNIL : la question de la sécurité

Dans son dernier rapport d'activité, la CNIL revient sur l'obligation de sécurité qui pèse sur les administrations et les entreprises et rappelle que celle-ci « a été renforcée par le RGPD et complétée de nouveaux outils comme la notification des violations, l'analyse d'impact sur la protection des données ou les codes de conduite ».

La CNIL souligne, d'ailleurs, que **la sécurité est un point systématiquement vérifié lors de procédures de contrôle,** que ce soit sur le respect des principes de base mais aussi sur la mise en place des nouveaux outils de conformité, notamment l'exigence d'un registre des violations de données.

La CNIL rappelle également que les manquements à l'obligation de sécurité figurent parmi **les manquements les plus couramment constatés** et précise que *« 2/3 des sanctions depuis 2017 incluent un manquement à la sécurité, et plus de 40 % des sanctions sont prises sur ce seul fondement ».*

Il est à noter que la majorité de sanctions prononcées en 2019 étaient fondées sur un manquement à l'obligation de sécurité (voir notre article « Rapport d'activité 2019 de la CNIL : focus sur les mises en demeure et sanctions »).

S'agissant de leur montant, celui-ci oscille **entre 15 000 et 400 000** euros et concernent des défaillances sur des points élémentaires de sécurité, à savoir :

- Données librement accessibles par modification des URL
- Politique de mot de passe non-conforme
- Transmission de mots de passe en clair
- Transmission de mots de passe par une connexion non-chiffrée (http)
- Absence de verrouillage automatique des sessions de poste de travail
- Un défaut de protocole de test afin de garantir l'absence de vulnérabilité avant la mise en production d'un nouveau développement

La CNIL annonce comme objectif pour l'année 2020, l'**amélioration du niveau minimal de sécurité des entreprises qui traitent des données à caractère personnel**.