aston avocats
BUSINESS PARTNERS

IP-IT - DATA PROTECTION

BILAN 2021 DES DÉLIBÉRATIONS DE LA CNIL EN MATIÈRE DE SANCTIONS

Décryptage par Anmar Lucia Pinto, Avocat

Le pouvoir de sanction de la CNIL

À l'issue de contrôles ou de plaintes, en cas de **méconnaissance des dispositions du RGPD ou de la loi Informatique et Libertés** de la part des responsables de traitement et des sous-traitants, la formation restreinte de la CNIL peut prononcer des **sanctions** à l'égard des responsables de traitements qui ne respecteraient pas ces textes.

Le montant des sanctions pécuniaires peut s'élever jusqu'à :

- **20 millions d'euros** ; ou
- **4 % du chiffre d'affaires** de l'entreprise.

Au cours de l'**année 2021**, il a été constaté une **augmentation** du nombre de sanctions particulièrement sévères et restrictives prononcées par la CNIL.

Comment se passe un contrôle de la CNIL ?

1. Qui la CNIL peut-elle contrôler ?

Toute société et/ou entité traitant des données à caractère personnel disposant d'un établissement en France.

2. Quels sont les contrôles de la CNIL ?

- **Le contrôle sur place :** une délégation de la CNIL se rend directement au sein des locaux d'un responsable de traitement ou d'un sous-traitant.
- **L'audition sur convocation :** un courrier est adressé au responsable de traitement ou au sous-traitant afin qu'un ou plusieurs représentants de la société se présentent dans les locaux de la CNIL.
- **Le contrôle en ligne :** les agents de la CNIL effectuent des vérifications en consultant notamment des données librement accessibles ou rendues accessibles directement en ligne, y compris par imprudence, négligence ou du fait d'un tiers.
- **Le contrôle sur pièces :** les agents de la CNIL adressent un courrier accompagné d'un questionnaire destiné à évaluer la conformité des traitements mis en œuvre par un responsable de traitement ou un sous-traitant.

3. Les étapes de la procédure de sanction

1. Origine du dossier

PLAINTES

CONTRÔLES
En ligne / sur place

VIOLATION DE DONNÉES

→ Procédure de sanction → Désignation d'un rapporteur + formation restreinte

2. Avant la séance

Un projet de rapport est rendu proposant les mesures de sanctions envisagées. Suite à cela, un échange d'observations intervient entre le rapporteur et la société.

3. Séance de formation restreinte

Pas de sanction

Sanction
- **Publique** communiquée sur les sites legifrance.gouv.fr et cnil.fr
- **Non-publique**
- **Pécuniaire**
- **Non-pécuniaire** (rappel à l'ordre, injonction sous astreinte, etc.)

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-003 du 12 janvier 2021 :

Parties : Ministère de l'Intérieur / CNIL

Contexte :

À la suite du confinement décidé par le Gouvernement au mois de mars 2020, plusieurs articles de presse ont fait état de l'utilisation par la police et la gendarmerie de drones équipés d'une caméra afin de veiller au respect des mesures prises dans ce contexte.

Le 7 mai 2020, le traitement potentiel des données personnelles qui pourraient être générées par l'utilisation de ces drones a donné lieu à l'initiation d'une procédure de contrôle de la CNIL à l'encontre du ministère.

Manquements :

La formation restreinte déclare l'existence des manquements suivants sur la base de l'activité menée par les forces de sécurité pendant les mois de confinement.

- **Manquement relatif à la licéité du traitement et à l'absence d'analyse d'impact :**

Traitement de données personnelles par le biais de **drones équipés d'une caméra** → **Risque élevé** pour les droits et les libertés des personnes physiques → **Analyse d'impact impérative**

- **Manquement relatif à l'information des personnes :**

Canal d'information pour les personnes concernées → Aucun dispositif n'a été prévu → **Manque de correspondance aux exigences légales**

Sur les mesures correctrices et leur publicité :

Privation de l'ensemble des garanties des personnes concernées dont elles auraient dû bénéficier →
- Information sur le traitement mis en place
- Information sur l'exercice des droits des personnes concernées

→ **Gravité du manquement**

Sanction :

Rappel à l'ordre + injonction de se mettre en conformité avec la loi Informatique et Libertés et le RGPD.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-008 du 14 juin 2021 (I) :

Parties : BRICO PRIVÉ / CNIL

Contexte :

Le 13 janvier 2021, une délégation de la CNIL procède à un contrôle en ligne de tout traitement accessible à partir du domaine bricoprive.com, édité par la société BRICO PRIVÉ. À l'issue de son instruction, le rapporteur nommé par la CNIL notifie à la société un rapport détaillant les manquements au RGPD qu'il estimait.

Manquements :

- **Manquement à l'obligation de définir et de respecter une durée de conservation des données à caractère personnel proportionnée à la finalité du traitement :**

  ✕ L'entreprise ne précise pas la période pendant laquelle les données personnelles doivent être conservées.

- **Manquement relatif à l'obligation d'informer les personnes :**

  ✕ Absence de lien entre les informations mises à la disposition des utilisateurs du site web et les dispositions de l'article 13 du RGPD, à savoir
  - les coordonnées du délégué à la protection des données ;
  - les durées de conservation ;
  - les bases juridiques des traitements ; et
  - les droits dont les personnes bénéficient au titre du RGPD.

- **Manquement relatif à l'obligation de respecter la demande d'effacement des données à caractère personnel :**

  ✕ Défaut de suppression des données par l'entreprise malgré les demandes des personnes concernées.

- **Manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel :**

  ✕ Non-respect des exigences de sécurité pour l'accès aux informations stockées sur le site web

  CNIL → Recommandation de mot de passe composé au minimum de 12 caractères contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

- **Manquement aux obligations relatives aux informations (cookies) stockées sur le terminal des utilisateurs :**

  ✕ Non-respect du devoir d'information aux utilisateurs et non-obtention de leur consentement avant de s'inscrire ou d'accéder aux informations.

- **Manquement relatif à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe :**

  ✕ Non-respect du devoir de recueillir le consentement préalable, libre, spécifique et éclairé des personnes créant un compte sur le site web.

Sur les mesures correctrices et leur publicité :

Six manquements ont été constatés → **Violation des principes fondamentaux du RGPD** } **Preuve de négligence grave**

Sanction :

500.000 € d'amende administrative + injonction de se mettre en conformité avec la loi Informatique et Libertés et le RGPD.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-010 du 20 juillet 2021 :

Parties : AG2R LA MONDIALE / CNIL

Contexte :

Le 29 octobre 2019, la CNIL a mené une opération de contrôle sur place au sein des locaux du groupe AG2R LA MONDIALE. Ce contrôle visait plus particulièrement les traitements de données à caractère personnel des clients et des prospects du groupe.

Manquements :

La formation restreinte a déclaré l'existence des manquements suivants :

- **Manquement à l'obligation de limiter la durée de conservation des données :**
  La société n'avait pas mis en œuvre dans ses systèmes les durées de conservation qu'elle avait définies dans son référentiel.

  ✕ Non-respect par l'entreprise des périodes de conservation définies dans le cadre de référence du groupe AG2R LA MONDIALE.

  RGPD : les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire à la finalité poursuivie.

- **Manquement à l'obligation d'information des personnes :**
  L'information fournie aux personnes démarchées téléphoniquement par des sous-traitants de la société ne comportait pas l'ensemble des éléments exigés par le RGPD.

  ✕ Non-respect de l'obligation d'information sur les traitements de données à caractère personnel effectués

  - *durée de conservation ;*
  - *existence des différents droits dont bénéficient les personnes ;*
  - *existence du droit de retirer son consentement à tout moment ; et*
  - *droit d'introduire une réclamation auprès d'une autorité de contrôle.*

Sur les mesures correctrices et leur publicité :

Atteinte aux principes fondamentaux du RGPD → Limitation de la durée de conservation des données ; Obligation d'informer les personnes concernées → **Négligence grave**

Facteurs augmentant la gravité → Le nombre élevé de personnes concernées ; La nature sensible des données conservées pendant des durées excessives

Sanction :

1.750.000 € d'amende administrative.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-012 du 26 juillet 2021 :

Parties : MONSANTO COMPANY / CNIL

Contexte :

En mai 2019, plusieurs médias ont révélé que la société MONSANTO détenait un fichier contenant les données personnelles de plus de 200 personnalités politiques, ou appartenant à la société civile (par exemple des journalistes, militants de la cause écologiste, scientifiques ou encore agriculteurs) susceptibles d'influencer le débat ou l'opinion publique sur le renouvellement de l'autorisation du glyphosate en Europe.

Dans le même temps, la CNIL a été destinataire de sept plaintes émanant notamment de personnes concernées par ce fichier.

Les contrôles effectués par la CNIL ont révélé que ce recensement avait été réalisé pour le compte de la société MONSANTO par plusieurs sociétés spécialisées dans les relations publiques et le lobbying, dans le cadre d'une importante campagne de représentation d'intérêts.

Manquements :

- **Manquement à l'obligation d'informer les personnes concernées :**
  La création de fichiers de contacts par les représentants d'intérêts à des fins de lobbying n'est pas, en soi, illégale. En revanche, ne peuvent figurer dans ce fichier que des personnes qui peuvent raisonnablement s'attendre, en raison de leur notoriété ou de leur activité, à être l'objet de contacts du secteur.

- **Manquement à l'obligation d'encadrer les traitements effectués pour le compte du responsable de traitement par un acte juridique formalisé :**
  En tant que responsable de traitement, la société MONSANTO avait l'obligation d'encadrer par un acte juridique la réalisation du traitement effectué pour son compte par son sous-traitant, notamment afin de prévoir des garanties concernant la sécurité des données. La CNIL a cependant relevé qu'aucun des actes conclus entre les deux sociétés ne comportait les mentions prévues à l'article 28 du RGPD.

Sur les mesures correctrices et leur publicité :

Manque d'information + manque d'acte juridique. → **Atteinte aux droits des personnes concernées.** → **Absence de contrôle sur l'utilisation de leurs données personnelles.**

Sanction :

400.000 € d'amende administrative.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-013 du 27 juillet 2021 :

Parties : SOCIÉTÉ DU FIGARO / CNIL

Contexte :

La CNIL, saisie d'une plainte, a effectué plusieurs contrôles entre 2020 et 2021 sur le site web d'actualités lefigaro.fr. Ces contrôles ont permis de constater que lorsqu'un utilisateur se rendait sur ce site, des cookies étaient automatiquement déposés sur son ordinateur par des partenaires de la société, sans action de sa part ou malgré son refus.

Manquements :

- **Manquement à l'article 82 de la loi « Informatique et libertés »**

Négligences mises en exergue

- Dépôt des cookies à finalité publicitaire lorsqu'un utilisateur se rend sur le site web, avant toute action de sa part et sans recueil de son consentement ;
- Impossibilité pour l'utilisateur de refuser de manière effective le dépôt des cookies à finalité publicitaire.

La société ne doit pas permettre le **dépôt des cookies** sur le terminal des utilisateurs lors de l'arrivée sur le site lefigaro.fr, **avant toute action de leur part et en l'absence de recueil de leur consentement.**

Le Figaro, en tant qu'éditeur du site web lefigaro.fr devait s'assurer que ses partenaires ne déposaient pas des cookies soumis au consentement avant que les utilisateurs aient fait le choix d'accepter ou de refuser.

Sur les mesures correctrices et leur publicité :

Non-respect aux exigences de l'article 82 de la loi Informatique et Libertés. → **Limitation aux utilisateurs d'exprimer la manière dont leurs données personnelles seront utilisées.**

Sanction :

50.000 € d'amende administrative.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-014 du 15 septembre 2021 :

Parties : Société nouvelle de l'annuaire français (SNAF) / CNIL

Contexte :

La CNIL a reçu seize plaintes, entre 2018 et 2019, indiquant des difficultés rencontrées lors de demandes d'effacement et de rectification de données personnelles.
Un contrôle en ligne et un contrôle sur audition ont permis de constater des manquements aux droits personnes concernées.

Manquements :

- **Manquement à l'obligation de respecter les demandes de rectification des données :**

La responsable du traitement est obligé de donner suite aux demandes de rectification des données stockées.

En cas de non-conformité → **Violation de l'article 16 du RGPD**

- **Manquement à l'obligation de respecter les demandes d'effacement des données :**

Le responsable du traitement doit respecter la demande d'effacement formulée par la personne concernée lorsque

- Elle s'est opposée au traitement de ses données à caractère personnel ;
- Le responsable de traitement ne démontre pas de motifs légitimes et impérieux justifiant le traitement.

- **Manquement à l'obligation de mettre en œuvre un registre des activités de traitement :**

Non-respect de l'article 30 du RGPD → La société est tenue de conserver un registre des activités de traitement effectuées sous la responsabilité du responsable du traitement.

- **Manquement à l'obligation de coopérer avec les services de la CNIL**

Non-respect de l'article 31 du RGPD → Le responsable du traitement et le sous traitant ainsi que, le cas échéant, leurs représentants sont tenus à coopérer avec l'autorité de contrôle dans l'exécution de leurs missions.

Sur les mesures correctrices et leur publicité :

La formation restreinte a constaté →
- **l'atteinte aux droits des personnes ; et**
- **le manque de coopération avec la CNIL.**

Sanction :

3.000 € d'amende administrative.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-016 du 24 septembre 2021 :

Parties : FAED / CNIL

Contexte :

Le FAED est un fichier de police judiciaire d'identification recensant les empreintes digitales de personnes mises en cause dans des procédures pénales. Ces empreintes sont principalement utilisées par les forces de l'ordre dans le cadre de leurs enquêtes.

Le 20 décembre 2019, la CNIL engage une procédure de contrôle pour vérifier le respect par le Ministère de l'intérieur de l'ensemble des dispositions légales européennes et nationales.

Manquements :

- **La conservation, dans le fichier, de données non prévues par les textes :**

  ✕ La CNIL a constaté que le nom d'une victime ou le numéro d'immatriculation d'un véhicule sont enregistrés dans le FAED, alors que ces informations ne font pas partie de celles pouvant être collectées.

- **Manquement relatif à la durée de conservation de données :**

  ✕ La CNIL a constaté que le point de départ des délais de conservation était calculé à compter de la dernière signalisation dans le FAED et non à compter de l'établissement de chaque fiche relative à cette personne.

- **Manquement relatif à l'exactitude des données :**

  ✕ Non-respect de l'obligation d'effacement des données en cas de relaxe ou d'acquittement définitif.

- **Manquement relatif à la sécurité des données :**

  ✕ La CNIL a constaté que les forces de police peuvent accéder au FAED en utilisant un mot de passe composé de 8 caractères. Or, compte tenu de la sensibilité des données qui figurent dans le FAED, ce type de mot de passe n'est pas suffisamment robuste.

- **Sur le manquement relatif à l'information des personnes :**

  ✕ La CNIL a relevé qu'aucune information n'est délivrée individuellement aux personnes dont les empreintes sont prises puis versées au FAED. Ainsi, les personnes concernées sont susceptibles d'ignorer jusqu'à l'existence même de ce fichier.

Sur les mesures correctrices et leur publicité :

- **Sensibilité des données traitées (données biométriques et d'infraction) ; et**
- **Grand nombre de personnes concernées (y compris, des mineurs).**

Sanction :

Rappel à l'ordre + injonction de se mettre en conformité avec la loi Informatique et Libertés et le RGPD.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-019 du 29 octobre 2021 :

Parties : RATP / CNIL

Contexte :

En mai 2020, la CNIL a été saisie par une organisation syndicale d'une plainte concernant la présence du nombre de jours de grève exercés par les agents dans les fichiers utilisés lors des procédures d'avancement de carrière. La CNIL a alors effectué des contrôles dans plusieurs centres de bus de la RATP qui ont permis de confirmer cette pratique illégale.

Manquements :

- **Manquement relatif à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données à caractère personnel traitées :**

✓ **RGPD** → Traitement des données personnelles
- **Adéquates**
- **Pertinentes**
- **Limitées**

✗ **RATP** → Stockage des données relatives au nombre de jours de grève des travailleurs.

La CNIL a relevé que ces données n'étaient pas nécessaires pour atteindre les finalités poursuivies.

- **Manquement à l'obligation de définir et de respecter une durée de conservation des données à caractère personnel :**

✓ **Finalité du traitement réalisé**
- **Suppression**
- **Anonymisation**
- **Archivage**

L'efficacité de la mise en œuvre d'une politique de conservation des données garantit que les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées.

- **Manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel :**
  - le responsable de traitement doit prendre les mesures appropriées pour assurer la confidentialité des données ;
  - l'accès aux données personnelles doit être limité aux personnes autorisées.

Sur les mesures correctrices et leur publicité :

Manquements aux principes fondamentaux du RGPD → **Preuve de défaillances graves en matière de protection de données à caractère personnel.**

Sanction :

400.000 € d'amende administrative.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-021 du 28 décembre 2021 :

Parties : FREE MOBILE / CNIL

Contexte :

Saisie de 19 plaintes, la CNIL a procédé à deux opérations de contrôle sur place dans les locaux de la société FREE puis de la société FREE MOBILE.
À l'issue de son instruction, des observations ont été formulées par la CNIL relatives aux manquements de la société FREE MOBILE.

Manquements :

- **Manquement à l'obligation de respecter le droit d'accès des personnes aux données à caractère personnel les concernant:**

  ✗ L'entreprise n'a pas traité la demande d'accès formulée par le plaignant, laquelle doit être traitée dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, conformément à l'article 12 paragraphe 4 du RGPD.

- **Manquement relatif à l'obligation de respecter la demande d'opposition des personnes concernées :**

  ✗ Dans le cadre des traitements de données à des fins de prospection commerciale, la CNIL sanctionne FREE MOBILE, sur le fondement des articles 12 et 21 du RGPD, de :
  - Ne pas avoir pris en compte l'opposition de la plaignante dans les délais prévus ; et
  - Ne pas avoir apporter une réponse à la demande d'opposition de la personne concernée, quand bien même elle ait été traitée.

- **Manquement relatif à l'obligation de protéger les données à caractère personnel dès la conception :**

  ✗ La CNIL rappelle que si des données peuvent être conservées à des fins déterminées, notamment d'exécution du contrat, à des fins comptables ou pour la gestion du contentieux, elles ne doivent pas être traitées dans le cadre de l'émission des facturations en cours alors que l'utilisation d'un identifiant permettant d'identifier le débiteur des différentes lignes mobiles pourrait être utilisé à la place.

  ✓ Des mesures techniques et organisationnelles auraient dues être prises dès la conception afin de procéder à l'effacement de données personnelles qui n'étaient plus nécessaires pour les besoins de la facturation.

- **Manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel :**

  ✗ La transmission par courriel, en clair, des mots de passe des utilisateurs méconnaît l'obligation de prendre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque prévue par l'article 32 du RGPD.

Sur les mesures correctrices et leur publicité :

Cinq manquements ont été constatés → **Violation des principes fondamentaux du RGPD** } **Preuve de négligence grave**

Sanction :

300.000 € d'amende administrative + publicité de la délibération pour une durée de deux ans à compter de sa publication.

Les sanctions prononcées par la CNIL en 2021

Délibération SAN-2021-023 du 31 décembre 2021 :

Parties : GOOGLE LLC et GOOGLE IRELAND / CNIL

Contexte :
Saisie de plusieurs plaintes dénonçant les modalités de refus des cookies sur les sites internet « google.fr » et « youtube.com », la CNIL a procédé à un contrôle en ligne le 1er juin 2021.
À l'issue de son instruction, la séance de la formation restreinte s'est tenue en présence des sociétés mises en cause.

Manquement :

- **Manquement relatif à l'obligation d'information d'un utilisateur d'un service de communications électroniques :**

  ✗ Les sociétés n'ont pas mis en œuvre les modalités de recueil du consentement des utilisateurs aux opérations de lecture et/ou d'écritures d'informations dans leur terminal (cookies et traceurs), en leur offrant un moyen de les refuser présentant une simplicité équivalente au mécanisme prévu pour leur acceptation, afin de garantir la liberté de leur consentement.

  ✓ Le principe : refuser des cookies doit être aussi simple que de les accepter.

  ✓ Les boutons « Accepter les cookies » et « Refuser les cookies » doivent apparaître au même moment et de la même manière afin de ne pas induire l'utilisateur en erreur.

Sur les mesures correctrices et leur publicité :

Un manquement a été constaté → **Violation de l'article 82 de la Loi Informatique et Libertés** } **Nécessité de garantir la liberté de consentement de l'utilisateur**

Sanction :

150.000.000 € d'amende administrative + injonction de se mettre en conformité avec la loi Informatique et Libertés.

Délibération SAN-2021-024 du 31 décembre 2021 :

Parties : FACEBOOK IRELAND LIMITED / CNIL

Contexte :
A la suite de quatre saisines, la CNIL a effectué un contrôle en ligne sur le site web « facebook.com ».

Manquements :

- **Manquement relatif à l'obligation d'information d'un utilisateur d'un service de communications électroniques : violation de l'article 82 de la Loi Informatique et Libertés**

Sanction :
60.000.000 € d'amende administrative + injonction de se mettre en conformité avec la loi Informatique et Libertés.