

# Thématiques prioritaires de contrôle 2023 : caméras « augmentées », applications mobiles, fichiers bancaires et dossiers patients

15 mars 2023

---

La CNIL effectue des contrôles sur la base de plaintes reçues, de l'actualité, mais également de thématiques prioritaires annuelles. En 2023, elle se concentrera sur l'utilisation de caméras « augmentées » par les acteurs publics, l'utilisation du fichier des incidents de crédit aux particuliers, la gestion des dossiers de santé et les applications mobiles.

Chaque année, la CNIL conduit des centaines de [contrôles](#) (345 en 2022) qui peuvent faire suite à des **plaintes**, des signalements de [violations de données](#) ou à des événements dans l'actualité.

La CNIL définit également des **thématiques prioritaires** afin d'orienter sa **politique de contrôle** sur des sujets à fort enjeu pour le public et pour évaluer la conformité des secteurs choisis.

## L'utilisation de caméras « augmentées » par les acteurs publics

Le développement de caméras dites « augmentées » ou « intelligentes », notamment par des collectivités territoriales, est l'objet de nombreuses questions régulièrement posées à la CNIL. Le recours à ces dispositifs est notamment prévu dans le cadre de manifestations sportives de grande ampleur prévues en 2023 (Coupe du monde de rugby) et en 2024 ([Jeux olympiques](#)).

La CNIL a fait de la thématique des usages des caméras « augmentées » un axe prioritaire de son [plan stratégique 2022-2024](#). Cela se traduit par la mise en œuvre d'une série d'actions qui comportent un accompagnement des acteurs privés et publics, mais aussi la réalisation de contrôles.

Ainsi, après avoir organisé une consultation publique dans le prolongement de laquelle elle [a pris position sur cette technologie](#), la CNIL a décidé de faire de ce sujet une thématique prioritaire de ses contrôles en 2023. Cela lui permettra de **vérifier le respect du cadre légal** par les acteurs publics.

## L'utilisation du fichier des incidents de remboursement de crédit aux particuliers

[Le fichier des incidents de crédit aux particuliers \(FICP\)](#) de la Banque de France recense les informations sur les incidents de paiement caractérisés liés aux découverts et aux crédits accordés pour des besoins non professionnels, ainsi que les informations relatives aux situations de surendettement. Sa consultation par les banques est obligatoire, notamment avant tout octroi de crédit.

Les inscriptions à ce fichier représentent donc un enjeu particulièrement fort, puisqu'elles peuvent constituer un frein pour les personnes dans leurs démarches ultérieures et leurs relations avec les banques. L'exactitude des données qui y figurent, leurs durées de conservation ainsi que le respect des conditions de gestion de ce fichier sont donc cruciaux.

Les contrôles porteront principalement sur **les conditions dans lesquelles les banques accèdent au fichier**, en **extraient des informations** et le **tiennent à jour** après régularisation des incidents de paiement.

## L'accès au dossier patient informatisé au sein des établissements de santé

La CNIL et le ministère en charge de la santé ont, ces dernières années, beaucoup échangé **sur la sécurité des données de santé**, par exemple concernant la politique générale de sécurité des systèmes d'information en santé (PGSSI-S), [le dossier médical partagé \(DMP\)](#), la carte de professionnel de santé (CPS-eCPS), le service « pro Santé connect », etc. Ces différents dispositifs ont ainsi fait l'objet de nombreuses demandes d'avis et de conseils.

La sécurité des données de santé, qui avait déjà été retenue comme thématique annuelle des contrôles de la CNIL en 2020 et en 2021, est une question récurrente que la CNIL rencontre dans un grand nombre de dossiers et qui concerne l'ensemble des établissements de santé.

Des vérifications ont déjà été engagées par la CNIL sur **l'accès au dossier patient informatisé (DPI)** en 2022 et se poursuivront en 2023.

Ce choix fait notamment suite à des plaintes reçues par la CNIL qui dénoncent des accès par des tiers non autorisés à des DPI au sein d'établissements de santé.

Les contrôles menés auront également pour objet d'examiner l'ensemble des mesures mises en place pour assurer la [sécurité des données](#).

# Le traçage des utilisateurs par les applications mobiles

Les fabricants de téléphones mettent à disposition des éditeurs d'application des identifiants permettant un suivi des utilisateurs pour des objectifs publicitaires, statistiques ou techniques (Apple IDFA, IDFA, Google AAID...). L'usage systématique de ces identifiants, équivalent « mobile » de l'utilisation massive des cookies sur les sites web, s'effectue bien souvent sans l'information ou le consentement des utilisateurs.

À la suite de la modification de la [recommandation sur l'utilisation de cookies et autres traceurs](#), plusieurs contrôles ont déjà été réalisés sur des applications qui accèdent aux identifiants générés par les systèmes d'exploitation mobiles en l'absence de consentement des utilisateurs. La CNIL poursuivra ses vérifications en 2023.

Pour rappel, la CNIL conduit [des travaux parallèles sur les bonnes pratiques en matière de développement des applications mobiles](#).

## Délégués à la protection des données (DPO) : des contrôles au niveau européen en 2023

À la suite d'un premier cadre d'application coordonné (*coordinated enforcement framework*) du Comité européen de la protection des données portant sur le *cloud* en 2022, la CNIL et ses homologues vont organiser une action similaire afin de procéder à des vérifications sur la désignation et les modalités d'exercice des fonctions de [délégué à la protection des données \(DPO\)](#).

En effet, les DPO jouent un rôle essentiel dans le respect effectif de la législation sur la protection des données et la promotion des droits des personnes concernées. Ils doivent ainsi bénéficier de ressources suffisantes et adaptées à l'accomplissement de leurs missions.

[Lire le communiqué de presse du CEPD](#)

Texte reference

## Pour approfondir

> [Comment se passe un contrôle de la CNIL ?](#)

> [Le contrôle de la CNIL](#)

> [FICP : Fichier national des Incidents de remboursement des Crédits aux Particuliers](#)

> [Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position](#)

> [Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation](#)

> [Applications mobiles : la CNIL présente son plan d'action pour protéger votre vie privée](#)

> [\[EN\] Priority topics for investigations in 2023: "smart" cameras, mobile apps, bank and medical records](#)