Les plaintes et les investigations année 2023

Les plaintes

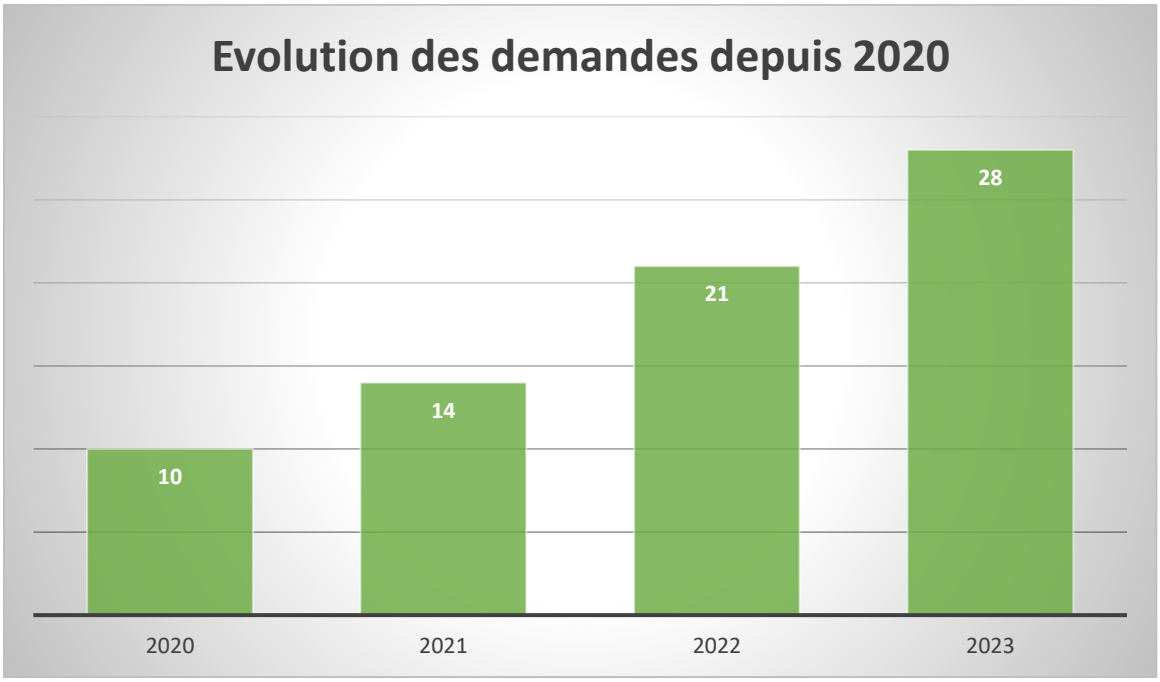
49 plaintes ont été adressées à la Commission en 2023, en augmentation par rapport à l'année précédente au cours de laquelle elle avait été saisie par 41 personnes.

Evolution du nombre total de plaintes adressées à la CCIN depuis 10 ans :

2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
51	17	11	15	13	15	24	19	28	41	49

Les plaintes liées à l'utilisation des réseaux sociaux

28 plaintes portant sur la suppression de contenus publiés en ligne ont été déposées en 2023 auprès de la CCIN, chiffre en constante augmentation chaque année. Ainsi par rapport à l'année 2021 le nombre de saisines a doublé.

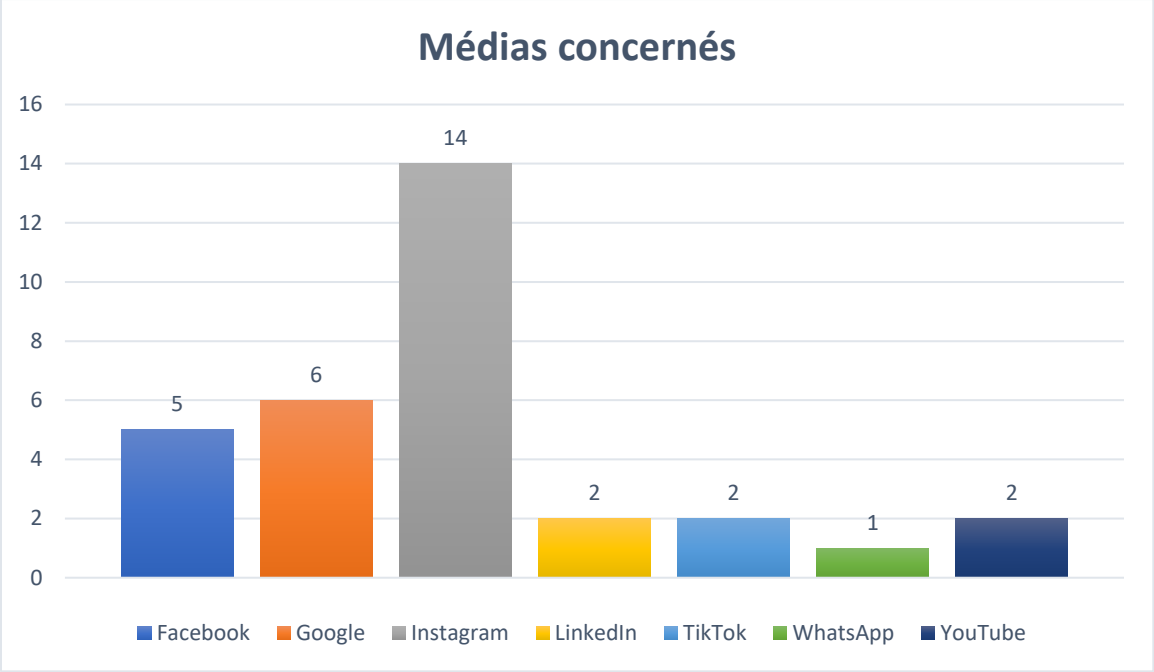


Sur ces 28 plaintes, 2 ont été classées sans suite :

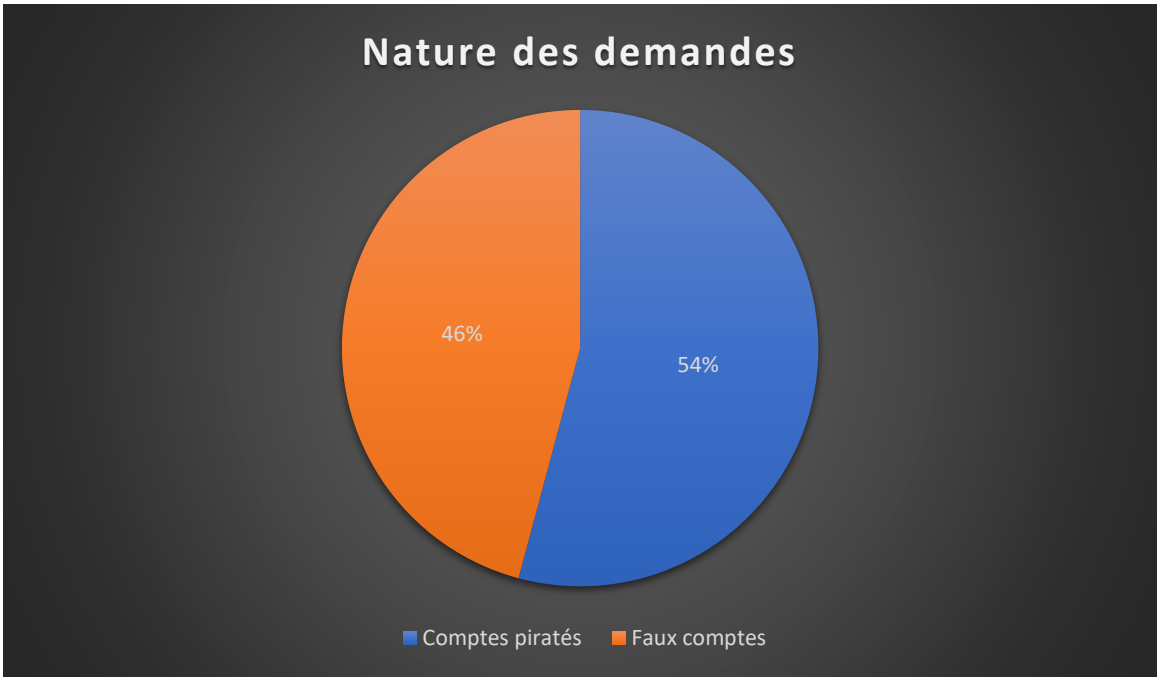
- la première a été résolue directement par le plaignant auprès de WhatsApp ;
- la seconde a été jugée irrecevable en raison d'une absence de lien avec les données personnelles et d'atteinte à la vie privée.

Facebook (5 plaintes) et Instagram (14 plaintes) ont été les principaux réseaux sociaux concernés par les saisines.

Certaines de ces plaintes concernaient des atteintes à la vie privée sur plusieurs médias.



Les demandes ont eu essentiellement pour objet la récupération de comptes piratés (13) et la suppression de faux comptes (11).



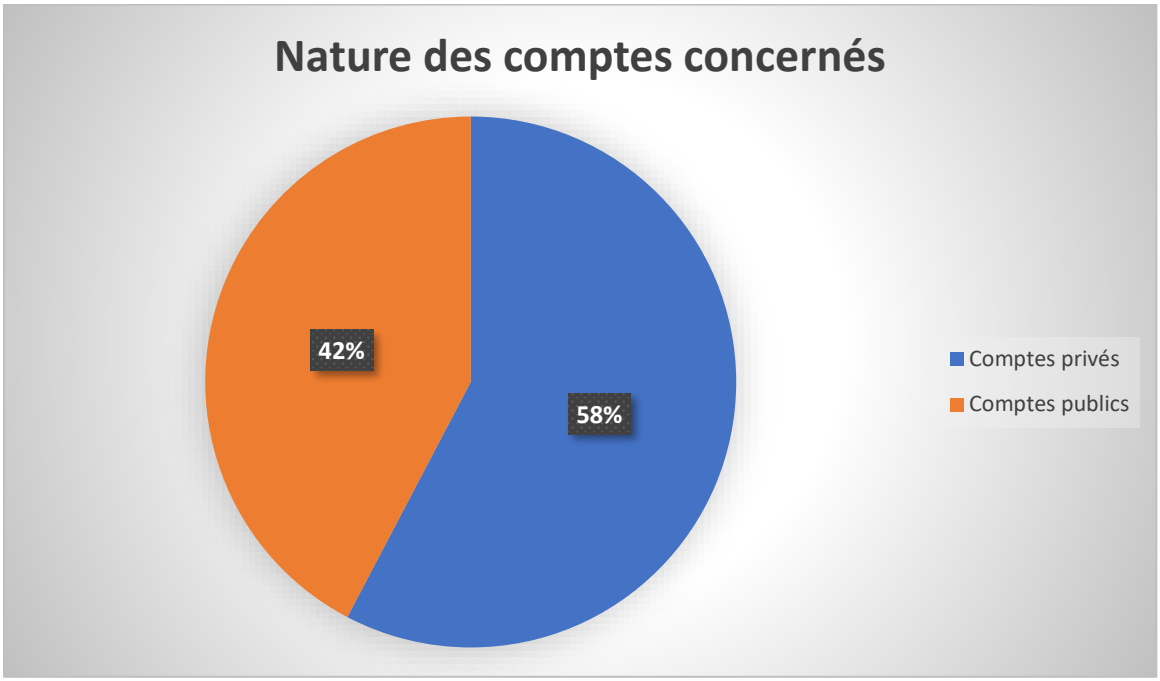
Qu'est-ce que le contrôle appelé « checkpoint » mis en place par Facebook pour les comptes usurpateurs ?

Ce système empêche les utilisateurs de se connecter à leurs comptes tant qu'ils n'ont pas réalisé une série d'étapes et d'actions. Les checkpoints sont utiles, par exemple, lorsqu'un compte semble être compromis, lorsque plusieurs tentatives de connexion ont échoué ou lorsque les conditions générales et politiques de Meta Platforms Ireland Limited, notamment les politiques en matière d'intégrité et d'authenticité, ont été enfreintes.

Lorsqu'un compte est soumis à un checkpoint, le titulaire de ce compte doit entreprendre des démarches pour faire vérifier son identité afin de récupérer l'accès audit compte et d'éviter que celui-ci ne soit désactivé de manière permanente.

Si le créateur du compte ne résout pas le checkpoint dans un délai de 30 jours, le compte en question sera alors désactivé de manière permanente et sa suppression sera programmée.

Par ailleurs, les comptes concernés par les demandes de récupération et de suppression étaient essentiellement privés (15).



Recrudescence des demandes de suppression de faux profils Instagram menant à des sites à caractère sexuel

La CCIN a pu constater une augmentation des demandes de suppression de faux comptes Instagram renvoyant vers des pages à connotation sexuelle. Le profil des

victimes est en général toujours le même : des jeunes femmes postant régulièrement des photos d'elles sur leur propre compte Instagram.

Ces photos ainsi que leurs nom et prénom sont ensuite repris par des personnes mal intentionnées afin de créer un faux profil Instagram sous un nom d'utilisateur très ressemblant à l'original.

En plus de cela, une biographie faisant la promotion de contenus pour adultes contient un lien vers une page à caractère sexuel créée sur Wix.

La CCIN ne peut que rappeler aux internautes l'importance de faire très attention aux photos qu'ils/elles partagent sur les réseaux sociaux.

Tout ce qui est posté sur les réseaux sociaux peut être réutilisé par des tiers à des fins malveillantes !

En cas de difficulté la CCIN se tient aux côtés des internautes pour obtenir la suppression de ces faux comptes et pages.

A cet égard, il convient de noter que la plateforme Wix prend très au sérieux ce problème et a mis en place un formulaire, très simple à remplir : Report Abuse \| General Abuse \| Wix.com

La fausse page est en général supprimée dans les heures qui suivent le signalement.

La CCIN a également traité cette année 2 demandes concernant le réseau social TikTok :

- la première portait sur la récupération d'un compte piraté ;
- la seconde avait pour objet la suppression de plusieurs photos récupérées depuis le compte Instagram de la personne concernée qui avaient été republiées sans son consentement sur TikTok.

En outre, la CCIN a dû intervenir auprès du réseau social professionnel LinkedIn pour obtenir la récupération de 2 comptes créés par des personnes physiques qui avaient été piratés.

Suite à l'intervention de la CCIN, tous ces comptes ont été, dans des brefs délais et en fonction des demandes, soit supprimés soit récupérés.

Très souvent, les piratages peuvent être résolus très facilement par les particuliers eux-mêmes en suivant tout simplement les procédures mises en place par les réseaux sociaux.

Aussi, la Commission encourage les plaignants à contacter dans un premier temps lesdits réseaux avant de la saisir ensuite uniquement en cas de démarches infructueuses.

Un petit guide des procédures de réinitialisation du mot de passe ou de récupération de compte figure dans la section « Fiches Pratiques » de notre site Internet.

La CCIN a été par ailleurs saisie de 2 demandes relatives à la plateforme YouTube :

- la première avait pour objet la récupération d'un compte professionnel piraté ;
- la seconde portait sur la suppression d'une vidéo diffusant des propos à caractère diffamatoire.

La Commission n'a toutefois pas pu intervenir directement auprès de YouTube qui souhaite que les personnes concernées agissent elles-mêmes, au moyen des procédures mises à leur disposition à partir de leur compte Google : **https://www.youtube.com/reportingtool/legal .**

La CCIN a également été saisie par un Service du Gouvernement concernant la publication d'une vidéo sur Facebook qui avait été bloquée pour cause de manquements présumés aux droits d'auteur. En effet, une chanson était diffusée dans la vidéo.

Après intervention de la Commission, le Service a pu conserver sa publication sur Facebook.

Enfin, la CCIN a dû agir auprès de Google pour solliciter le déréférencement de différents contenus publiés sur le moteur de recherche. Les demandes concernaient :

- une Ordonnance Souveraine prononçant la révocation d'un fonctionnaire ;
- plusieurs articles diffusant des propos à caractère diffamatoire concernant des résidents de la Principauté.

Malheureusement, ces plaintes n'ont pas abouti. A cet égard, la Commission constate qu'il devient de plus en plus difficile d'obtenir le déréférencement des articles en cause par le moteur de recherche.

Ce dernier justifie son choix de ne pas procéder au déréférencement des articles en se fondant notamment sur les motifs suivants :

- l'activité même de Google qui est de rassembler et de classer des informations publiées en ligne, sans aucun contrôle sur les contenus publiés par les sites eux-mêmes ;
- l'auteur de la publication, notamment lorsqu'elle émane d'une Autorité administrative et que cette publication est permanente ;
- l'intérêt que peuvent présenter les informations pour le public.

En cas de diffamation présumée, le meilleur moyen pour résoudre des questions relatives à l'exactitude des déclarations, contenues dans un article ou toute autre publication, est la procédure judiciaire.

Google a mis en ligne un formulaire à l'attention des personnes qui font l'objet de propos à caractère diffamatoire, qui doivent agir directement : https://support.google.com/legal .

Par ailleurs, Facebook met à la disposition des personnes concernées un « Formulaire de signalement pour diffamation » leur permettant de signaler directement une publication qu'elles jugent diffamatoire.

Les caméras de vidéosurveillance

La CCIN a été saisie à 5 reprises concernant l'exploitation de dispositifs de vidéosurveillance. 4 de ces saisines ont donné lieu à des contrôles en 2023 [1]

La 5ème plainte a concerné un immeuble d'habitation pour lequel il a été porté à la connaissance de la Commission que des caméras étaient en cours d'installation, et que certaines d'entre elles permettraient de filmer les couloirs d'accès aux logements, et dans certains cas, les portes d'entrée des appartements, ce que la CCIN interdit formellement pour des raisons tenant à l'indispensable préservation de la vie privée des résidents et de leurs visiteurs.
Suite à l'intervention de la CCIN les caméras concernées n'ont pas été installées.

L'utilisation d'outils de communication en lien avec le milieu professionnel

3 plaintes ont concerné en 2023 l'utilisation d'outils de communication, soit par le biais de messageries électroniques sur le lieu de travail, soit par la communication à l'employeur de conversations sur un chat privé.

- Comme les années précédentes, la CCIN a dû intervenir auprès d'employeurs pour la **non désactivation des adresses emails nominatives** d'anciens salariés.

  Saisie à 2 reprises, son intervention a permis de faire cesser l'exploitation de ces adresses de messagerie. A cette occasion elle a demandé à ce qu'une procédure soit mise en place au sein des entités concernées.

Messagerie électronique : les bonnes pratiques à adopter en cas de départ définitif d'un salarié

La CCIN est de plus en plus souvent contactée par d'anciens salariés qui constatent que leur adresse email nominative professionnelle est encore active alors qu'ils ont quitté leurs fonctions depuis plusieurs mois.

Aussi elle souhaite préciser les bonnes pratiques à adopter.

[1] Voir infra : les investigations

- Lors du départ définitif d'un salarié sa boite email nominative doit être « *bloquée* » c'est à dire qu'elle ne doit plus pouvoir recevoir d'emails, ni en envoyer, à l'exception d'un message automatique qui sera adressé à chaque personne ayant envoyé un email à l'adresse concernée.

Ce message automatique a vocation à informer l'expéditeur de l'email que son interlocuteur ne travaille plus au sein de l'entité, et qu'il devra désormais envoyer ses emails à telle ou telle adresse. Ceci pourra être pratiqué pendant 3 mois au maximum, selon les fonctions et le degré de responsabilité de l'ancien salarié.

- A l'échéance de cette période l'adresse email nominative de l'ancien salarié sera désactivée (supprimée).

- L'employeur doit permettre au salarié de récupérer les emails privés susceptibles de se trouver dans sa boite email nominative professionnelle.

→ ***Ces principes concernent toutes les messageries électroniques***

- Des employés d'une société avaient créé un **Chat privé** sur leurs téléphones personnels, afin de discuter d'un projet de restructuration de leur entreprise. L'un d'entre eux ayant informé la Direction du contenu de cette discussion, et des salariés y ayant participé, la CCIN a été saisie par certains de ces salariés, et a également été consultée par la Direction qui était sollicitée afin de savoir quel salarié l'avait informée. Les salariés ayant saisi la CCIN souhaitaient qu'elle leur communique le nom du salarié qui avait informé la Direction de l'existence et du contenu de cette discussion.

  La réponse de la CCIN a été claire : l'employeur ne peut en aucune façon tirer des conséquences de cette conversation privée dont il n'aurait pas dû avoir connaissance, et la CCIN a bien évidemment refusé d'avoir accès au contenu de ce Chat privé, et de rechercher le salarié qui avait donné les informations à l'employeur.

Les difficultés en matière d'exercice des droits

Conformément à l'article 13 de la Loi n° 1.165 toute personne physique a le droit d'accéder aux informations la concernant et d'obtenir qu'elles soient modifiées s'il y a lieu, l'article 15 venant pour sa part préciser que la réponse à une demande d'accès doit s'effectuer sous un délai d'un mois. Il est en outre précisé que les informations doivent être communiquées au demandeur *« sous forme écrite, non codée et conforme au contenu des enregistrements ».*

Des difficultés récurrentes en matière de droit d'accès

Saisie sur le fondement du droit d'accès la Commission a eu à connaître de 4 plaintes en 2023.

L'intervention de la CCIN a été l'occasion de rappeler certains **principes en matière de réponse à une demande de droit d'accès :**

* en l'état des dispositions légales monégasques le droit d'accès ne confère pas à son titulaire un droit à obtenir copie de l'ensemble des documents le concernant ;

*la réponse à une demande de droit d'accès doit se faire en respectant les droits des tiers : le droit d'accès ne doit pas être un moyen pour le demandeur d'obtenir des informations personnelles sur des tiers ;

* une copie (en noir et blanc, barrée) d'un document d'identité ne peut être demandée que lorsqu'il existe des doutes sur l'identité de la personne faisant valoir son droit d'accès.

Dès la résolution de ces problématiques liées au droit d'accès, 2 des plaignants ont saisi la CCIN de 3 plaintes distinctes, portant sur la transmission de leurs données à des tiers.

La rectification des données transmises à des tiers

L'article 16 de la Loi n° 1.165 dispose que :

« La personne intéressée peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou supprimées les informations la concernant lorsqu'elles se sont révélées inexactes, incomplètes, équivoques, périmées ou si leur collecte, leur enregistrement, leur communication ou leur conservation est prohibé.

Sur sa demande, copie de l'enregistrement de l'information modifiée lui est délivrée sans frais.

S'il y a eu communication à des destinataires, l'information modifiée ou sa suppression doit leur être notifiée, sauf dispense accordée par le Président de la commission de contrôle des Informations Nominatives ».

Dans ce cadre la CCIN est intervenue afin qu'un plaignant obtienne la suppression des informations transmises par erreur à un tiers.

Les 2 autres plaintes ont concerné des communications d'informations à un tiers situé dans un pays étranger, et pour lesquelles le plaignant a également saisi l'Autorité de protection des données personnelles dudit pays. Ces plaintes ont donné lieu à une intervention de la CCIN auprès des entités ayant transmis ces informations, afin de connaître l'éventuel fondement légal à cette transmission. Ces plaintes étaient toujours en cours d'instruction en fin d'année 2023.

La désindexation de contenus publiés au Journal Officiel

La CCIN a été saisie à 2 reprises par des personnes ayant fait l'objet de mesures de révocation, publiées au Journal Officiel de Monaco, et non désindexées par le site Internet concerné malgré le nombre d'années écoulées depuis la publication de ces

mesures (6 ans pour la plus ancienne). De ce fait les résultats effectués sur les moteurs de recherche à partir de leurs noms faisaient apparaitre ces mesures de révocation, rendant ainsi extrêmement difficiles leurs recherches d'emplois. Face au refus de l'exploitant du site de procéder à cette désindexation, la CCIN a été saisie par les plaignants.

En dépit des échanges intervenus avec l'exploitant de ce site Internet, celui-ci a opposé une fin de non-recevoir à la CCIN, refusant totalement de prendre en compte les arguments tirés notamment de la jurisprudence de la Cour Européenne des Droits de l'Homme en matière de droit à l'oubli numérique, et de droit au respect de la vie privée et familiale, comprenant notamment la réputation de la personne concernée.

Par ailleurs saisis par la CCIN d'une demande de déréférencement, les moteurs de recherche n'y ont pas donné suite dans la mesure où les mesures de révocation étaient accessibles depuis un site Internet officiel.

Au-delà des seuls cas des 2 plaignants, la CCIN a décidé d'adopter une délibération portant recommandation sur cette question, afin de tenter d'obtenir une inflexion de la position de la part de l'exploitant du site internet du Journal de Monaco. Cette recommandation devrait être publiée en 2024.

Le traitement des données

La CCIN a été saisie de 2 plaintes en lien avec une problématique de traitements illicites de données qui auraient eu lieu il y a plusieurs années, au-delà du délai de prescription en matière délictuelle, ce qui a conduit la CCIN à s'interroger sur l'applicabilité des délais de prescription.

L'exploitation de sites Internet

Les 2 plaintes reçues en 2023 ont concerné :

- l'exploitation d'un site Internet dont, après recherches, il est apparu que l'exploitant était dans un pays tiers. Le plaignant a été invité à se rapprocher de l'Autorité de contrôle dudit pays ;

- la détermination du responsable de traitement du site Internet d'un commerce dont 2 entités revendiquaient l'exploitation. Sans entrer dans le différend commercial entre ces 2 entités, la CCIN est intervenue auprès du responsable de traitement du site Internet concerné afin qu'il le régularise auprès d'elle, ce qui a été fait.

Les investigations : les caméras de vidéosurveillance toujours au centre des enjeux de préservation de la vie privée

La Commission a diligenté 4 investigations en 2023, toutes en lien avec l'exploitation de dispositifs de vidéosurveillance.

L'une d'entre elle a concerné un établissement du secteur public. Les 3 autres ont, en revanche, été réalisées auprès d'entités du secteur privé.

Ces 4 contrôles ont fait suite à des signalements, toutefois, conformément aux articles 18-1 et 18-2 de la Loi n° 1.165, modifiée, seules les investigations effectuées au sein d'établissements privés ont préalablement fait l'objet d'une Ordonnance sur requête délivrée par le Président du Tribunal de Première Instance afin de garantir l'accès aux locaux professionnels privés concernés. En effet le droit d'opposition ne concerne pas, en application de ces articles, les locaux publics.

Lors de ces 4 contrôles, aucun dispositif n'avait fait l'objet de formalités préalables auprès de la CCIN, ce qui démontre le peu de maîtrise et de connaissance dans l'utilisation de systèmes de vidéosurveillance qui peuvent être particulièrement intrusifs pour les personnes qui y sont soumises.

L'utilisation de WhatsApp pour envoyer des images de caméras de vidéosurveillance

La Commission a reçu un signalement en 2023 portant sur l'utilisation d'un système de vidéosurveillance au sein d'un **établissement du secteur public.**

Aucun avis favorable n'ayant été émis par la Commission pour la mise en œuvre de ce traitement, il a été décidé de procéder à une investigation sur place.

Lors de l'arrivée dans les locaux de l'établissement, les Agents, assermentés, désignés par le Président de la Commission ont constaté que l'un des membres du personnel était en train de filmer, à l'aide d'un téléphone portable, l'écran de contrôle du système de vidéosurveillance.

Interrogé à ce sujet, ce dernier leur a indiqué procéder au visionnage des enregistrements vidéos de la veille afin de relever d'éventuels incidents. En cas d'incident, il a indiqué procéder au film de l'enregistrement concerné et à son envoi, *via* l'application mobile WhatsApp, aux membres d'un groupe créé pour effectuer un contrôle des incidents. Ce dernier faisait par la suite remonter toute survenue d'incident à la Direction de tutelle sans que les vidéos concernées ne soient jointes.

Par ailleurs, il a été constaté que certaines des caméras exploitées par l'établissement public permettaient de capturer des images de la voie publique de manière incidente ainsi que celles de la sortie d'un parking privé et de passants.

Enfin, il a été noté qu'aucun affichage ne permettait d'informer les personnes concernées de l'existence d'un dispositif de vidéosurveillance au sein de l'établissement.

Conformément aux dispositions de l'article 19 de la Loi n° 1.165 susvisée, un rapport d'investigation a été adressé au responsable des locaux en toute fin d'année 2023 afin

de relever les irrégularités à la Loi qui ont été constatées lors des opérations de contrôle.

Ce dossier devrait être clôturé en 2024.

Les investigations effectuées auprès **d'entreprises du secteur privé** ont eu lieu sur la base d'éléments permettant de soupçonner des irrégularités à la Loi n° 1.165 du 23 décembre 1993, modifiée.

Elles se sont dès lors déroulées sur le fondement de l'article 18-2 de la Loi susvisée, après autorisation du Président du Tribunal de Première Instance et sans que les responsables des locaux ne puissent faire valoir leur droit d'opposition.

La surveillance permanente, continue et en temps réel des personnes concernées

L'attention de la Commission a été portée sur la possible exploitation de systèmes de vidéosurveillance, possiblement équipés de micros, contrairement aux dispositions de sa délibération n° 2010-13 portant recommandation sur les dispositifs de vidéosurveillance mis en œuvre par les personnes physiques ou morales de droit privé.

Les Agents en charge de procéder à l'investigation ont constaté la présence d'une caméra autonome connectée au Wifi de l'établissement. Cette dernière était placée au-dessus d'un espace accueillant des clients.

Le dispositif, directement géré *via* l'interface installée sur le téléphone portable du responsable des locaux, comportait en outre une fonction audio ce qui permettait à ce dernier de bénéficier d'un accès continu et en temps réel aux images et à la sonorisation.

Il a également été relevé qu'aucun affichage ne permettait d'informer les personnes concernées de la présence d'un système de vidéosurveillance au sein de l'établissement. Le responsable des locaux a toutefois indiqué aux Agents qu'un tel affichage existait mais que ce dernier, initialement présent sur la porte d'entrée, était tombé sans avoir été réinstallé. Une affiche représentant un pictogramme de caméra a été présentée aux Agents. Cette dernière a été réinstallée.

Le Rapport relevant les irrégularités constatées lors des opérations de contrôle a été notifié au responsable des locaux en fin d'année 2023 afin qu'il puisse y répondre dans un délai d'un mois.

Eu égard à l'atteinte importante portée à la vie privée des personnes concernées dont les conversations pouvaient être écoutées, en temps réel et de façon continue, le Président de la CCIN se prononcera, à l'issue du délai d'un mois précité, sur les suites à donner à ces irrégularités.

Une investigation au sein de plusieurs établissements appartenant à deux sociétés

La Commission a procédé à des opérations de vérification au sein de l'ensemble des établissements détenus par deux sociétés.

A cet égard, il a été constaté, au sein de l'un d'entre eux, la présence d'une caméra fixe non branchée et d'un câble d'alimentation coupé. Plusieurs traces, laissant supposer le déploiement d'un ancien système, ont également pu être observées sur les murs de cet établissement.

Le responsable des locaux concernés a attribué la présence du système ainsi que des traces au commerce ayant précédemment occupé les locaux.

Il a été précisé, par le responsable des locaux des autres établissements, que des systèmes de vidéosurveillance avaient pu être exploités par le passé mais que tel n'était plus le cas au moment de l'investigation.

Des vérifications additionnelles ont été diligentées au sein de plusieurs des établissements. Certaines divergences, au niveau des explications apportées par les responsables des locaux lors des opérations de contrôle initiales, ont pu être constatées. Il a cependant été décidé de procéder à la clôture des opérations d'investigation. En outre, le retrait du dispositif non branché a par ailleurs été demandé au responsable de traitement.

L'exploitation de caméras mobiles à des fins de dissuasion

La Commission a reçu une plainte portant sur la présence de caméras au sein de la vitrine d'un commerce. Ces caméras étaient orientées de telle façon qu'elles permettaient de filmer la vitrine du commerce voisin.

Lors des opérations d'investigation, les Agents investigateurs ont relevé la présence de deux systèmes autonomes de vidéosurveillance : un système fixe et un système composé de deux caméras portables. Ces dernières étaient gérées directement *via* une interface installée sur le téléphone portable du responsable des locaux.

Le responsable des locaux a indiqué que le système de caméras portables avait été installé à des fins de dissuasion sans être exploité en pratique. Il indiquait à cet égard avoir supprimé l'application permettant le pilotage des caméras.

Le système fixe a, quant à lui, fait l'objet d'une demande d'autorisation de la Commission, conformément aux dispositions de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 modifiée.

Dans le cadre du courrier de transmission de sa délibération portant autorisation à la mise en œuvre de ce traitement, la Commission a toutefois rappelé au responsable de traitement que cette autorisation ne concerne que les caméras mentionnées dans le dossier de demande d'autorisation. Elle a rappelé que l'exploitation de caméras en dehors du périmètre de cette autorisation constituerait une non-conformité à la Loi n° 1.165 susvisée.

Les opérations d'investigations étaient toujours en cours en fin d'année 2023 s'agissant du système de caméras portables.