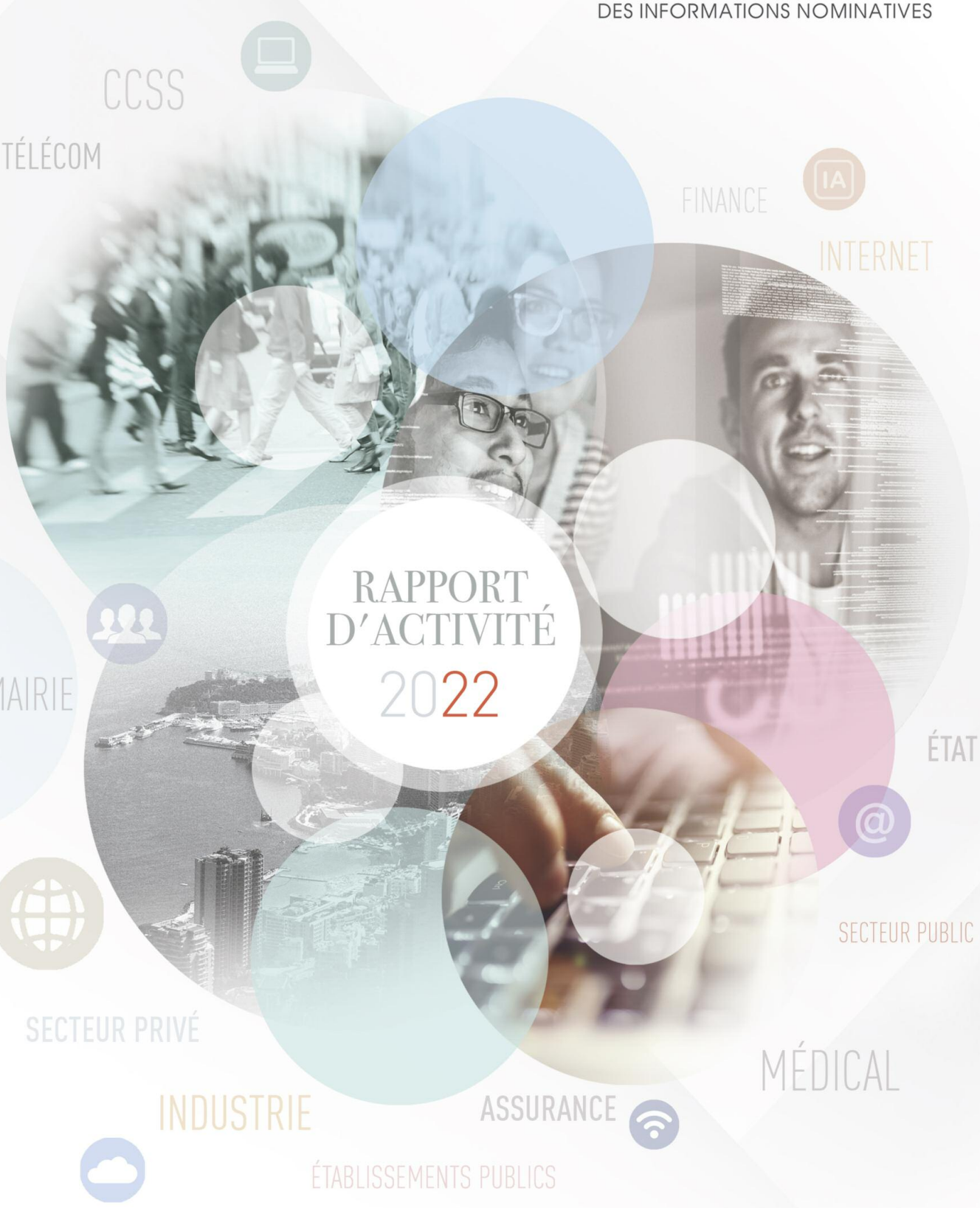
CCIN

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES




# RAPPORT D'ACTIVITÉ 2022

14ème rapport public

CCIN

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

# Le message du Président

« *A trente ans, tout est joué : œuvre, carrière, amour, destinée. Après, il suffit de suivre les rails - chemin de velours ou mauvaise glissade, peu importe - on suit sa pente. Entre vingt et trente ans, on la fait* »[1] .

Le 23 décembre 2023, peu après la diffusion du présent rapport d'activité, la CCIN aura désormais 30 ans. Et s'il est évident que cette citation ne la concerne pas, une certaine analogie peut être de mise, et je crois pouvoir affirmer que notre Commission est sur de bons « *rails* ».

Service du Gouvernement lors de sa création en 1993 et principalement consultée pour donner des avis plutôt confidentiels, la CCIN est devenue 15 ans plus tard une Autorité Administrative Indépendante dotée de pouvoirs de recommandation, de contrôle et de sanction. Entre 20 et 30 ans, effectivement, elle a donc tracé son chemin. Ainsi, son activité est chaque année plus soutenue et traversée par de nouveaux défis, comme en atteste le présent rapport d'activité qui démontre l'engagement continu en 2022 de la Commission dans la protection des droits et libertés fondamentaux des personnes concernées.

La CCIN est-elle pour autant sur un « *chemin de velours* » ?

Pour répondre à cette question, il convient de rappeler la volonté affichée par le Gouvernement Princier de doter « *la Principauté d'un niveau de protection adapté aux nouvelles exigences européennes en matière de protection des données à caractère personnel de sorte à ce qu'une décision dite « d'adéquation » soit rendue par la Commission européenne, facilitant par là même les transferts de données avec les pays de l'Union européenne* ».

Cette volonté résulte du retard de notre droit interne en matière de protection des informations nominatives eu égard aux nouveaux standards européens. Dès lors, pour que Monaco puisse se voir reconnaitre ce statut, il faut que la CCIN poursuive encore plus avant son « *chemin* » : publicité étendue de ses avis, pouvoirs de sanction proportionnés mais aussi plus dissuasifs, et une nouvelle organisation qui en soit le reflet, tant pour les responsables de traitement que pour les personnes concernées.

Aussi, le projet de Loi n° 1.054 relative à la protection des données personnelles, dont il vous est fait mention depuis le rapport d'activité 2020, a pour vocation d'introduire ces changements indispensables. Ils devraient je l'espère être effectifs en 2024.

Le chemin de la protection des informations nominatives se poursuivra donc vraisemblablement sans la CCIN, mais avec l'ADPD, Autorité de Protection des Données Personnelles, qui viendra la remplacer.

Gageons ainsi que pour éviter la « mauvaise glissade », les principales problématiques du projet de Loi évoquées dans le rapport d'activité 2021 seront levées, car le chemin de l'adéquation ne peut être parcouru par la seule Autorité de contrôle, mais avec l'ensemble des parties prenantes, notamment dans les domaines les plus intrusifs que sont le secteur Police/Justice, et celui en lien avec la préservation de la sécurité nationale.

Si l'année 2022 montre une baisse significative des saisines sur des projets de textes, alors que certains d'entre eux auraient pu, ou dû, lui être soumis par le Gouvernement, elle est également marquée par un nombre sans cesse croissant de plaintes reçues par notre Commission, attestant ainsi d'une prise de conscience de la part des particuliers concernant les enjeux liés à la protection de leurs données personnelles.

Elle démontre surtout la nécessité de dialogue pour résoudre des problématiques sans cesse plus complexes et pointues, qui nécessiteraient parfois une intervention législative ou règlementaire : articulation du droit d'accès aux informations nominatives et du droit d'accès aux documents administratifs, définition du périmètre des dispositifs de lanceur d'alerte, poursuite des modifications textuelles relatives à la lutte contre le blanchiment de capitaux, ou encore encadrement des outils de surveillance et de suivi des comportements tels que notamment les dispositifs de prévention de fuites de données confidentielles, dont l'utilisation est en progression constante, et qui sont techniquement toujours plus poussés.

CCIN ou APDP, le chemin à vos côtés est encore long et riche d'échanges. L'Autorité en charge de la protection des données personnelles saura, je n'en doute pas, continuer son « *chemin* » en remplissant ses nouvelles missions avec détermination, en étant toujours à l'écoute des entités de la Principauté, tout en veillant avec fermeté à la protection des droits et des libertés individuelles.

Guy MAGNAN

[1] Citation de Pierre De Boisdeffre.

RAPPORT D'ACTIVITÉ PUBLIÉ EN APPLICATION DE L'ARTICLE 2-14 DE LA LOI N° 1.165 RELATIVE À LA PROTECTION DES INFORMATIONS NOMINATIVES

# Sommaire

5

6



*Les articles 4 et 5 de la Loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives disposent que la Commission de Contrôle des Informations Nominatives est composée de six membres nommés par Ordonnance Souveraine pour une durée de cinq ans, renouvelable une fois.*

*En application de ces dispositions, les Commissaires ont été nommés par l'Ordonnance Souveraine n° 7.468 du 14 mai 2019, qui a renouvelé 5 Commissaires sur les 6 qui avaient été nommés en 2014.*

# LA COMPOSITION DE LA COMMISSION

De gauche à droite : Rainier Boisson, Vice-Président ; Guy Magnan, Président ; Florestan Bellinzona, Commissaire ; Jean-François Cullieyrier, Commissaire ; Robert Chanas, Commissaire ; Philippe Blanchi, Commissaire.

## GUY MAGNAN

**Président**

Diplômé en gestion et en commerce Guy Magnan débute une carrière d'enseignant et mène en parallèle une activité libérale au sein d'un Cabinet d'expertise comptable.

En 1980 il prend en charge l'intendance du Lycée Technique de Monte-Carlo puis intègre la Société Monégasque de l'Electricité et du Gaz en 1983 dont il deviendra Administrateur Directeur Général en 1995.

En 1998, il est également nommé Président Délégué de la Société Monégasque d'Assainissement.

Elu au sein du Conseil National de 1978 à 2003, il a été successivement Président de la Commission des Intérêts Sociaux et des Affaires Diverses, Président de la Commission de Législation et Président de la Commission du Logement.

Au cours de ses mandats d'élu il a également assuré la Vice-Présidence de la Délégation de la Principauté auprès de l'Organisation pour la Sécurité et la Coopération en Europe (OSCE).

En juin 2013 il est nommé Membre de la CCIN sur proposition du Conseil National, et accède à la Présidence de la Commission en juin 2014, après avoir été nommé sur proposition du Ministre d'Etat.

En juin 2019 son mandat de Membre de la CCIN est renouvelé pour 5 ans sur présentation du Ministre d'Etat et il est à nouveau élu en qualité de Président de la Commission.

Homme d'écoute et de dialogue, sa parfaite connaissance de la Principauté, de ses Institutions et de son tissu économique lui permet d'aborder les dossiers avec pragmatisme, tout en veillant à la préservation des droits et libertés de chacun.

Guy Magnan est également Membre du Conseil de la Couronne depuis le 19 avril 2018, nommé sur présentation du Conseil National.

## RAINIER BOISSON

**Vice-Président**

Architecte diplômé de l'Ecole des Beaux-Arts, Urbaniste diplômé de l'Ecole Nationale des Ponts et Chaussées et de l'Institut d'Urbanisme de Paris, Rainier Boisson ouvre son Cabinet d'architecte en 1976.

Empreint des affaires publiques dès son plus jeune âge grâce à son père qui fut Maire de Monaco durant 16 ans, il est élu Conseiller National de 1978 à 2003 et devient Président de la Commission de la Jeunesse en 1994.

Au cours de son Mandat il a également été Président de la section monégasque de l'Assemblée Parlementaire de la Francophonie. Consul Honoraire de Finlande à Monaco depuis 1988, ces différentes fonctions lui ont permis de parfaire sa connaissance du fonctionnement des relations et des Institutions internationales.

Désigné Membre de la CCIN en juin 2014 sur proposition du Conseil National, il en a été élu Vice-Président à cette même période, pour une durée de cinq ans au cours de laquelle la Commission bénéficie de son analyse rigoureuse empreinte de sa forte sensibilité à la protection des droits de l'homme et des libertés fondamentales.

En juin 2019 son mandat de cinq ans est renouvelé sur présentation du Conseil National.

A cette occasion il est à nouveau élu en qualité de Vice-Président de la Commission.

Il est également Membre du Conseil du patrimoine depuis le mois d'octobre 2018.

## Florestan BELLINZONA

**Commissaire**

Titulaire d'une maîtrise en droit privé filière carrières judiciaires, Florestan Bellinzona débute un troisième cycle Police, Gendarmerie et Droits fondamentaux de la personne avant d'intégrer l'Ecole Nationale de la Magistrature de Bordeaux.

Après une expérience de six mois au Bureau Permanent de la Conférence de La Haye de droit international privé, il est nommé Juge suppléant en octobre 2003 puis Juge en 2005 avant d'accéder aux fonctions de Premier Juge en 2013.

Ayant été successivement Juge des accidents du travail, Juge tutélaire en charge des affaires familiales puis Juge de l'application des peines, il est actuellement Président de la formation correctionnelle statuant sur intérêts civils, Président de la formation correctionnelle pour mineurs et préside les audiences de flagrant délit ainsi qu'une partie des audiences correctionnelles. Il est également Vice-Président du Tribunal de Première Instance depuis octobre 2020.

Désigné Membre de la Commission en juin 2014 sur proposition du Directeur des Services Judiciaires, sa pratique quotidienne de la résolution des contentieux et son attrait pour l'informatique donnent à la Commission une vision pertinente de l'application du droit dans un contexte de complexification et de généralisation des nouvelles technologies.

Son mandat a été renouvelé au mois de juin 2019, sur proposition du Directeur des Services Judiciaires.

## Philippe BLANCHI

**Commissaire**

Diplômé en droit public et en droit international, Philippe Blanchi intègre l'Administration en 1968 au Secrétariat du Conseil National dont il sera Secrétaire Général de 1976 à 1988.

Nommé Secrétaire Général de la Direction des Relations Extérieures en 1989, il est appelé en 1990 au Cabinet de S.A.S. le Prince Souverain dont il sera Chargé de Mission puis Conseiller en 1996. De manière concomitante il dirige le Bureau de Presse du Palais pendant plusieurs années.

De 2004 à 2012 il occupe différents postes diplomatiques en qualité d'Ambassadeur de Monaco en Suisse puis en Italie ; il sera depuis Rome le premier Ambassadeur de Monaco à Saint Marin, en Slovénie, en Croatie et en Roumanie. Durant cette période, il assure également la Représentation permanente de la Principauté près de l'Office des Nations Unies et des Organisations Internationales basées à Genève et l'Organisation des Nations Unies pour l'Alimentation et l'Agriculture, ainsi que du Programme Alimentaire Mondial à Rome.

Nommé Membre de la CCIN en juin 2014 sur proposition du Conseil d'Etat, et renouvelé au mois de juin 2019, également sur présentation du Conseil d'Etat, il apporte à la Commission son expérience diversifiée du fonctionnement des Institutions nationales et internationales acquise dans ses différentes fonctions.

## Robert CHANAS

**Commissaire**

Titulaire d'un Diplôme d'Etudes Supérieures Spécialisées à l'Institut d'Administration des Entreprises de Nice et d'une maîtrise de sciences économiques, Robert Chanas débute sa carrière en 1982 au sein du Service Administratif et Financier de Radio Monte Carlo en tant que contrôleur de gestion.

Il occupera successivement les postes de responsable du personnel, de responsable du budget et du contrôle de gestion, d'adjoint au Directeur Financier et de Directeur Administratif et Financier en charge de la gestion des sociétés du groupe à partir de 1994.

En 2001, il devient Directeur Administratif et Financier de la nouvelle Société d'Exploitation des Ports de Monaco. Il met en place toute la structure d'administration et de gestion de l'entreprise (paye, comptabilité, informatique et gestion des places de port).

A partir de 2004, il rejoint les Caisses Sociales de Monaco en tant qu'Attaché de Direction, puis de Fondé de Pouvoir de l'Agent Comptable en début 2007.

La même année, il devient Agent Comptable.

Il intègre la CCIN en avril 2021 sur proposition du Conseil Communal, et la fait bénéficier de sa parfaite connaissance du fonctionnement de la Sécurité Sociale en Principauté pour les secteurs du Commerce, de l'Industrie et des Travailleurs Indépendants concernant notamment les procédures de déclarations sociales, et de son expérience de l'organisation et de l'administration des entreprises.

## Jean-François CULLIEYRIER

**Commissaire**

Diplômé de droit public et de sciences politiques, Lauréat de la Faculté de Droit de Paris, Jean François Cullieyrier est également ancien élève de l'Institut d'Etudes Politiques et de l'Institut des Hautes Etudes Internationales de la Faculté de Droit de Paris.

En 1977, il débute sa carrière professionnelle en Principauté en tant que Directeur de la succursale de la Banque Rothschild, avant d'être nommé Directeur Général du Crédit Commercial de France à Monaco.

La même année, il intègre l'Association Monégasque des Activités Financières dont il est actuellement Vice-Président et trésorier.

En 2001, il devient Administrateur, Directeur Central d'HSBC Private Bank, puis nommé en 2018 Vice-Président du Conseil d'Administration de la Banque J. Safra Sarasin (Monaco) SA.

Sa parfaite connaissance du secteur bancaire et financier l'a conduit à être nommé Vice-Président de la Commission de Contrôle des Activités Financières, fonction qu'il assume depuis 2007.

Il siège également au Tribunal du Travail, au Comité Directeur du Monaco Economic Board, au Comité de Contrôle de la Caisse de Compensation des Services Sociaux ainsi qu'à la Commission des Jeux dont il est Président depuis 2007.

Il intègre la CCIN en juin 2019 sur présentation du Conseil Economique et Social dont il a été membre à partir de 1989 puis Président de la Section financière jusqu'en 2012.

1

# LES MISSIONS ET LE FONCTIONNEMENT DE LA COMMISSION

**La Commission de Contrôle des Informations Nominatives créée par la Loi n° 1.165 du 23 décembre 1993 est chargée de veiller au respect des libertés et droits fondamentaux des personnes dans le domaine des informations nominatives.**

Le dispositif législatif mis en œuvre par la Loi du 23 décembre 1993 a été largement remanié en 2008 afin que la protection des informations nominatives, garantie par le droit interne monégasque, soit en adéquation avec les standards européens tels qu'ils sont encadrés par la Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel relatif aux Autorités de contrôle et aux flux transfrontières de données.

Les standards internationaux ayant évolué à la suite de la modernisation de la Convention 108, et de l'entrée en application du Règlement Général sur la Protection des Données (RGPD) de l'Union européenne, le cadre législatif monégasque a lui aussi vocation à être modifié très prochainement.

Les missions de la Commission sont définies à l'article 2 de la Loi n° 1.165 du 23 décembre 1993, modifiée. Celles-ci sont nombreuses et témoignent de l'importance de la protection des données à caractère personnel dans la vie des acteurs de notre société.

## Une Mission d'information

**Au travers de la publication :**

- **de ses délibérations portant avis ou autorisation sur la mise en œuvre de traitements ;**
- **du rapport annuel d'activité ;**
- **de ses recommandations sur des sujets spécifiques ;**
- **de communiqués et de fiches pratiques sur son site Internet www.ccin.mc.**

## Une mission de contrôle

L'article 18-1 de la Loi n° 1.165, introduit par la Loi n° 1.420 du 1er décembre 2015, définit le cadre des investigations « *préventives* », que la CCIN mène de sa propre initiative.

Dans ce cas, a été prévue la possibilité pour les responsables de locaux professionnels privés de faire valoir leur droit de s'opposer aux opérations d'investigation ; celles-ci ne pourront alors se

dérouler que sur autorisation du Président du Tribunal de Première Instance auquel il revient d'apprécier le motif ou l'absence de motif justifiant l'opposition.

Pour sa part, l'article 18-2 de la Loi n° 1.165 prévoit une procédure spécifique lorsqu'il existe une raison de soupçonner que la mise en œuvre des traitements n'est pas conforme à la Loi sur la protection des informations nominatives, sans que le droit d'opposition puisse être invoqué, mais uniquement sur autorisation préalable du Président du Tribunal de Première Instance. L'Ordonnance permettant aux investigateurs d'accéder aux locaux peut faire l'objet d'un recours non suspensif. S'il est fait droit à ce recours, le juge peut alors déclarer la nullité des opérations d'investigation.

## Une mission d'exercice des droits d'accès des personnes concernées

Régi par l'article 15-1 de la Loi n° 1.165, le droit d'accès indirect permet à toute personne concernée de saisir la Commission afin qu'elle accède, pour son compte, aux informations nominatives la concernant, auxquelles elle ne peut, en vertu de dispositions légales, accéder directement.

Ce droit d'accès indirect concerne en premier lieu les informations nominatives traitées par les autorités judiciaires ou administratives dans le cadre de traitements :

- intéressant la sécurité publique ;
- relatifs aux infractions, condamnations ou mesures de sûreté ;
- ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

Ce même droit s'applique également aux informations traitées par les organismes assujettis à la Loi n° 1.362 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, relatives aux obligations de vigilance, de déclaration et d'information auprès du Service d'Information et de Contrôle sur les Circuits Financiers, devenu Autorité Monégasque de Sécurité Financière.

## Des sanctions administratives

Le Président de la Commission peut adresser à un responsable de traitement en cas de manquements à ses obligations :

- **un avertissement ;**
- **une mise en demeure de mettre fin aux irrégularités ou d'en supprimer les effets.**

Ces sanctions peuvent faire l'objet d'une publication.

## Le budget de la Commission

Pour l'année 2022 la Commission a bénéficié d'un budget total de **1.512.300,00 €** se répartissant ainsi :

- **947.300,00 €** au titre des crédits de fonctionnement, dont plus de la moitié est consacrée au paiement du loyer de ses locaux ;
- **565.000,00 €** au titre de ses dépenses salariales, en diminution par rapport à l'année précédente. Afin d'anticiper l'évolution de ses missions, la CCIN a demandé une modification de son organigramme dans le but de renforcer ses compétences.

## Le Secrétariat Général de la Commission

Pour remplir ses missions, la Commission est assistée d'un Secrétariat Général dont le fonctionnement et la coordination des Services sont de la responsabilité du Secrétaire Général.

Outre le Secrétaire Général, les Services de la Commission sont composés d'un Chargé de Mission spécialisé en ingénierie et en sécurité des systèmes, de cinq juristes ayant des domaines de compétences spécifiques, d'un informaticien et de deux Agents administratifs.

Le Secrétaire Général, le Chargé de Mission, l'informaticien, ainsi que trois juristes sont assermentés afin de procéder aux missions d'investigation.

Le Secrétariat Général sert d'intermédiaire entre les responsables de traitements, les personnes concernées et la Commission.

Il a notamment pour missions :

- **de s'assurer de la tenue et de la mise à jour du répertoire des traitements ;**
- **de gérer les consultations du répertoire public ;**
- **d'élaborer les projets de rapports d'analyses techniques et de délibérations de la Commission ;**
- **de répondre aux questions des responsables de traitements et de les accompagner dans leurs démarches auprès de la Commission ;**
- **d'informer et de conseiller toute personne intéressée par la protection des informations nominatives ;**
- **d'instruire les plaintes et les déclarations, demandes d'avis ou demandes d'autorisation ;`**
- **d'animer des réunions de sensibilisation ;**
- **d'assurer le secrétariat des séances de la Commission et des suites à donner à celles-ci.**

# 5

# LA CCIN ET LES DROITS DES PERSONNES CONCERNÉES

## Les consultations du répertoire public des traitements

L'article 10 de la Loi n° 1.165 offre la possibilité à toute personne physique ou morale de consulter le répertoire public des traitements.

Les informations figurant dans ledit répertoire sont les suivantes :

- **la date de la déclaration, de la demande d'avis ou de la demande d'autorisation relative à la mise en œuvre d'un traitement ;**

- les mentions portées sur celle-ci, à l'exception des mesures prises pour assurer la sécurité du traitement et des informations ;
- la dénomination du Service chargé de l'exploitation du traitement ;
- la date de délivrance du récépissé de la déclaration, de l'avis de la Commission ou de son autorisation ;
- les dates et libellés des modifications apportées aux traitements initiaux ;
- la date de suppression du traitement et celle, lorsqu'il y a lieu, de la radiation de l'inscription.

Au cours de l'année 2022 ce répertoire a été consulté 4 fois par des sociétés, ou par des Cabinets de conseil pour le compte de leurs clients, afin de faire le point sur les traitements qui ont déjà fait l'objet de formalités préalables, dans la perspective de poursuivre, ou d'initier, la mise en conformité.

## Les plaintes

41 plaintes ont été adressées à la Commission en 2022, en très forte augmentation par rapport à l'année précédente au cours de laquelle elle avait été saisie par 28 personnes.

**Les plaintes liées à l'utilisation des réseaux sociaux, d'Internet et d'applications mobiles**

L'article 16 de la Loi n° 1.165 confère à toute personne le droit d'exiger que les informations

nominatives la concernant soient rectifiées, complétées, clarifiées, mises à jour ou supprimées lorsqu'elles se sont révélées inexactes, incomplètes, équivoques ou périmées. L'essentiel des plaintes a concerné des demandes de suppression de contenus publiés sur des réseaux sociaux.

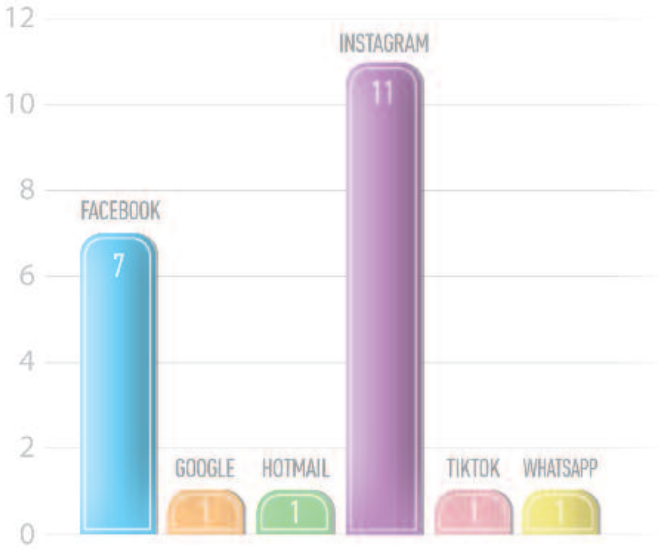
***La suppression de contenus en ligne***

En 2022, 21 plaintes portant sur le droit de suppression de contenus publiés en ligne ont été déposées auprès de la CCIN, soit 7 de plus qu'en 2021.

Sur ces 21 plaintes, 3 ont été classées sans suite :

- la première a été résolue directement par le plaignant auprès de WhatsApp avant même que la CCIN n'ait eu à intervenir ;
- la deuxième a été jugée irrecevable en raison d'une absence de lien avec les données personnelles et d'atteinte à la vie privée ;
- la troisième concernait une demande d'argent par message et a été classée sans suite faute d'éléments suffisants pour la traiter.

Médias concernés




Facebook (7 plaintes) et Instagram (11 plaintes) ont été les principaux réseaux concernés par les demandes de suppression.

En outre, la CCIN a traité pour la première fois une demande de récupération d'un compte TikTok qui a été piraté suite à un changement du numéro de téléphone associé.

A cet égard, il est important de noter que certaines des plaintes déposées concernaient des atteintes à la vie privée sur plusieurs médias.

Les demandes ont eu essentiellement pour objet la récupération de comptes piratés (19) et la suppression de faux comptes (3).

Les demandes relatives à la suppression des faux comptes concernaient :

- une haute personnalité de la Principauté dont 2 profils sur Facebook et sur Instagram reprenaient le nom, le titre ainsi que la photo officielle induisant en erreur les utilisateurs ;
- une page reprenant un jeu concours organisé par une personne morale afin de solliciter des contributions financières de la part des clients de ladite société pour y participer.

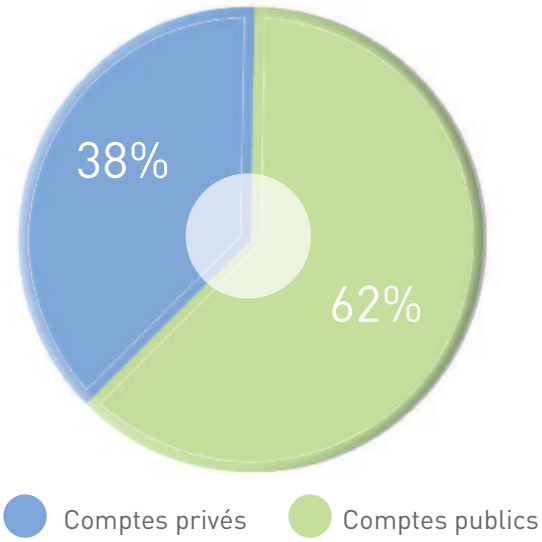
***Quid de la violation des droits de propriété intellectuelle ?***

Instagram indique que ses conditions d'utilisation n'autorisent pas la publication de contenu qui viole les droits de propriété intellectuelle de quelqu'un d'autre, y compris les droits d'auteur et les marques de commerce.

Si la personne concernée estime qu'un autre compte viole ses droits de propriété intellectuelle, Instagram recommande de soumettre un rapport à https://help.instagram.com/535503073130320

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

**Nature des comptes concernés**




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

Très souvent, ces problèmes de piratages peuvent être résolus 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 à la fin de ce rapport d'activité ainsi que dans la section « *Fiches Pratiques* » de notre site Internet.

La CCIN a également obtenu pour le compte d'une famille résidant en Principauté le déréférencement de plusieurs articles accessibles depuis le moteur de recherche Google. Les plaignants avaient également sollicité l'aide de la CCIN afin d'obtenir la suppression d'une publication diffamatoire sur un compte Facebook mais cette plainte n'a pas abouti.

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 de la personne concernée un « *Formulaire de signalement pour diffamation* » lui permettant de signaler directement une publication qu'elle juge diffamatoire.

Enfin, pour la première fois, la CCIN a été contactée dans le cadre d'une annonce de vente en ligne, qui a été récupérée frauduleusement sur deux sites marchands pour tenter d'escroquer des acquéreurs potentiels alors que le bien avait déjà été vendu. Il a alors été conseillé au plaignant de demander à ces deux sites le retrait immédiat de cette annonce frauduleuse, ce qui a été fait aussitôt. Aussi la CCIN n'a pas eu à intervenir.

**Les applications mobiles**

Une plainte a été déposée suite la réception d'une notification sur une application mobile, indiquant à la personne concernée qu'elle était bien réinscrite dans son association, alors que son dossier de réinscription avait été refusé quelques semaines avant. En effet cette notification mentionnait qu'un compte au nom de l'intéressé avait été créé. Toutefois celui-ci n'avait pas été en mesure de remettre son dossier d'inscription définitif, contenant l'ensemble des documents nécessaires, ainsi que de payer les frais d'inscription.

Dans un contexte conflictuel avec cette association, le plaignant redoutait que cette « *fausse inscription* » ait été faite délibérément par l'encadrement de cette dernière, afin de pouvoir mener à son terme une procédure disciplinaire initiée quelques semaines plus tôt.

La Commission a décidé de mener une mission de contrôle afin de vérifier si cette inscription résultait, ou non, d'un acte malveillant de la part de l'encadrement. (Voir infra : les investigations).


**Les plaintes liées au milieu professionnel**

En 2022 au total 11 plaintes ont émané de salariés ou d'anciens salariés, pour dénoncer des pratiques portant atteinte à leurs droits.

- 6 d'entre elles concernaient la messagerie professionnelle d'anciens salariés dont l'adresse email nominative n'avait pas été désactivée plusieurs semaines après leur départ. Le risque est alors qu'un autre salarié l'utilise en se faisant passer pour son ancien collègue, mais également que des messages à caractère personnel reçus sur cette adresse email soient lus par d'autres personnes que le destinataire, lequel a quitté l'entreprise.

Suite à l'intervention de la CCIN les adresses emails nominatives concernées ont été désactivées très rapidement par l'employeur. Dans un seul cas la CCIN n'est pas intervenue dans la mesure où l'ancien salarié qui l'avait saisie n'a pas répondu à ses questions visant à s'assurer que son ancien employeur exerçait bien à Monaco, et non en France, auquel cas il lui incombait de se rapprocher de la CNIL, et non de la CCIN.

***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.

- 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 professionnelles qu'elles soient utilisées à des fins de surveillance ou non.

L'une de ces 6 plaintes portait également sur le défaut de mise à jour du site Internet d'une société, laissant croire qu'un ancien salarié faisait toujours partie des effectifs car son nom apparaissait toujours au titre des collaborateurs. Là aussi l'intervention de la CCIN a permis le retrait de cette mention, devenue obsolète.

***Site Internet et informations relatives aux collaborateurs : les rappels importants !***

S'il est courant que des sites Internet disposent d'une rubrique dédiée à la présentation de certains de leurs collaborateurs, ces informations doivent être strictement limitées à leur vie professionnelle et pertinentes au regard de leurs fonctions.

Attention : il ne peut pas être imposé à un salarié de mettre sa photo en ligne : ceci doit résulter d'un choix librement exprimé par lui !

De plus ne pas oublier de retirer immédiatement les informations obsolètes en cas de départ d'un salarié.

• La CCIN a également été saisie par un entrepreneur dont l'adresse email professionnelle a été piratée aux fins d'envoi d'emails d'hameçonnage en nombre. Il lui a été conseillé de demander à son administrateur SI de réinitialiser son mot de passe et d'en saisir un autre réputé fort (caractères alphanumériques, spéciaux, avec changement de casse), le mot de passe initial n'étant en effet pas suffisamment robuste.

- Une autre plainte a émané d'un ancien salarié dont l'accès à son ordinateur professionnel lui a été refusé au motif que son employeur redoutait une fuite de données professionnelles. La CCIN a ici joué un rôle de « *médiateur* » et de « *tiers de confiance* » afin de restituer les données personnelles au plaignant.

- 2 plaintes ont concerné l'utilisation de caméras sur le lieu de travail. Dans les 2 cas les dispositifs de vidéosurveillance avaient été autorisés par la CCIN, mais était en cause l'utilisation des images afin de surveiller le travail des salariés.

Dans le premier cas il a été décidé de procéder à une mission de contrôle qui a été initiée en toute fin d'année, pour se poursuivre en 2023.

Dans le second cas l'intervention rapide de la CCIN a permis de faire retirer les images du dossier disciplinaire des salariés concernés.

- Une nouvelle fois la CCIN a eu à connaître de dysfonctionnements dans l'exploitation du dispositif de gestion des courses de taxis, dont l'Etat a délégué la gestion technique au même prestataire depuis de longues années. La CCIN est intervenue directement auprès du Service de l'Etat en charge de cette question, et a rencontré le nouveau prestataire afin de le sensibiliser dès le départ sur les bonnes pratiques qu'il se devait de respecter en sa qualité de gestionnaire technique du dispositif.

**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* ».

Saisie sur le fondement de ces droits d'accès et de rectification, la Commission a eu à connaître de 6 plaintes en 2022.

***L'accès aux documents administratifs versus le droit d'accès aux données***

L'articulation et les différences, en matière d'accès aux documents administratifs et d'accès aux données personnelles, ont été l'enjeu d'une plainte reçue en 2022.


***L'accès aux documents administratifs versus le droit d'accès aux données***

L'accès aux documents administratifs est régi par l'Ordonnance Souveraine n° 3.413 du 29 novembre 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, et plus particulièrement ses articles 22 à 27.

En application de ces dispositions toute personne peut demander la consultation de tout document administratif n'ayant pas fait l'objet d'une diffusion publique. Il n'est toutefois pas fait droit aux demandes trop imprécises. Sont également rejetées notamment les demandes portant sur des documents administratifs dont la consultation porterait atteinte au déroulement de procédures introduites devant des juridictions ou d'opérations préliminaires à de telles procédures.

Suite à une demande d'accès à un document administratif, une copie du document peut être adressée au demandeur. La consultation, ou la transmission de la copie, du document s'effectue toutefois après que les mentions portant atteinte notamment au secret médical, au secret des correspondances, à la vie privée, ... aient été biffées.

A la différence du droit d'accès aux données personnelles, qui concerne l'accès aux données du demandeur ou de ses enfants mineurs, l'accès aux documents administratifs peut concerner des documents relatifs à des tiers.

Le droit d'accès s'exerce relativement aux données personnelles et non à leur support, ce qui a pour conséquence que la copie d'un document ne peut être exigée, en application de la Loi n° 1.165. S'il est possible d'adresser au demandeur une copie des documents, sous réserve des droits des tiers, ceci ne constitue pas une obligation mise à la charge des responsables de traitements, lesquels peuvent tout aussi bien communiquer le contenu des documents, ainsi que les métadonnées y relatives (date de réception/d'envoi, service émetteur/destinataire, ...).

La Commission a été saisie de la plainte d'une personne souhaitant obtenir copie de l'intégralité du dossier établi par une entité publique concernant son enfant mineur et lui-même. Dans son courrier de demande, elle invoquait la Loi n° 1.165 relative à la protection des informations nominatives (qui ouvre le droit d'accès aux données), mais réclamait la transmission de la copie du dossier de son enfant mineur.

L'entité concernée lui ayant opposé un refus fondé sur l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, il a saisi la CCIN sur le fondement de l'article 15 de la Loi n° 1.165 relative à la protection des informations nominatives, régissant le droit d'accès aux données.

Malgré des échanges entre l'entité concernée et la Commission, le refus de communication a été maintenu sur le fondement de l'article 24 de l'Ordonnance Souveraine précitée qui permet le rejet des demandes de communication portant sur des documents administratifs dont la consultation porterait atteinte au déroulement de procédures introduites devant les juridictions ou d'opérations préliminaires à de telles procédures, dès lors que le dossier objet de la demande avait été transmis à l'Autorité judiciaire compétente par le service concerné.

En l'absence de doctrine et de jurisprudence la Commission a considéré que ce motif de refus n'était pas justifié dès lors que les documents litigieux demeuraient des documents administratifs et non judiciaires et, qu'à supposer applicable la réserve édictée par Ordonnance Souveraine, celle-ci ne pouvait être avancée pour s'opposer à l'exécution d'un droit prévu dans la Loi, compte tenu du respect de la hiérarchie des normes. Elle a estimé que certaines des informations nominatives sollicitées par le demandeur auraient dû lui être communiquées, sous réserve des droits des tiers, et de l'intérêt supérieur de son enfant.

Cette plainte a mis en exergue les lacunes du droit monégasque en la matière à défaut d'articulation


entre les textes relatifs la protection des informations nominatives régis par une Loi et ceux concernant l'accès aux documents administratifs qui ne résultent que d'une Ordonnance Souveraine, ainsi qu'en l'absence d'un organisme indépendant chargé de statuer sur la délivrance des documents administratifs.

La Commission ne peut que regretter cet état de fait et les conséquences qui en découlent pour les personnes concernées et s'interroge sur l'opportunité d'initier une réflexion dans ce domaine afin de préserver les droits fondamentaux des administrés tout en prenant en considération les autres intérêts en présence comme par exemple ceux des tiers ou d'autres personnes concernées par la communication sollicitée.

Les échanges intervenus en fin d'année 2022 avec l'entité concernée n'ayant pas abouti à faire droit à la demande du plaignant, qui plus est sur le fondement d'une base juridique qui ne le permet pas, le dossier devrait donner lieu à une sanction en 2023.

***Le droit d'accès et de rectification dans le domaine bancaire***

2 plaintes relatives au droit d'accès ont concerné des établissements bancaires.

La première plainte concernait tout à la fois une non réponse à une demande de droit d'accès, et une problématique de droit à l'ouverture d'un compte bancaire, institué à Monaco par la Loi n° 1.492 du 8 juillet 2020 relative à l'instauration d'un droit au compte. Sans se prononcer sur ce point qui n'est pas de son ressort, la Commission est intervenue auprès de l'établissement bancaire afin qu'il fasse droit à la demande d'accès formulée par le plaignant, ce qui a été fait dans les jours qui ont suivi.

Dans le second cas, l'établissement bancaire refusait de communiquer les informations d'une personne décédée à sa fille, au motif que celle-ci ne justifiait pas de sa qualité d'héritière de son père par la communication d'un document officiel authentifié par un notaire. Sur ce point, la Commission a appelé l'attention de l'établissement sur les dispositions en vigueur en matière d'accès aux informations des personnes décédées, régies par l'article 13 de la Loi n° 1.165 :

« *Sauf dispositions législatives contraires, l'ascendant, le descendant jusqu'au second degré, ou le conjoint survivant d'une personne décédée, peut, s'il justifie d'un intérêt, exercer les droits [d'opposition, d'accès et de rectification], pour ce qui est des informations concernant cette personne* ».

En application de ces dispositions, et considérant le fait que l'intérêt était ici de faire valoir ses droits dans la succession de son père, l'établissement a finalement donné suite à cette demande de droit d'accès.

Par ailleurs 1 plainte a concerné la rectification d'informations obsolètes. Le plaignant avait reçu un courrier d'un établissement bancaire dont il n'était plus client, lui indiquant que dans le cadre de l'échange automatique d'informations en matière fiscale, les données le concernant allaient être transmises aux Autorités fiscales de 2 pays étrangers. Le plaignant ne disposant plus depuis longtemps de résidences dans ces 2 pays, la CCIN a fait rectifier immédiatement les informations obsolètes, avant qu'elles ne soient transmises.

***L'accès à ses données professionnelles***

La plainte concernait ici les difficultés d'accès, par la personne concernée, à ses données personnelles dans le cadre de rapports d'incidents établis à son encontre. La non réponse à ce droit d'accès avait été justifiée, auprès de la CCIN, par le fait que plusieurs demandes de droit d'accès relatives aux informations du plaignant avaient été adressées au responsable de traitement, mais ces différentes demandes émanaient d'emails envoyés depuis différentes adresses qui n'étaient pas au nom du plaignant. Aussi il lui a été demandé d'adresser une copie de sa pièce d'identité (en noir et blanc et barrée) afin que le responsable de traitement puisse s'assurer de l'identité du demandeur.

***La suppression des données en matière de prospection commerciale***

1 plainte a concerné un défaut de désinscription d'un listing de prospection commerciale, résultant de l'utilisation, par le repreneur de l'entité concernée, d'une ancienne liste établie par le précédent propriétaire. Après avoir reconnu cette erreur, le responsable de traitement a retiré le nom du plaignant de ce listing.


***La législation en matière de prospection commerciale : Loi n° 1.383 du 2 août 2011, modifiée, pour une Principauté numérique***

*« Article 11.- Est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'un consommateur qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.*

*Toutefois, la prospection directe par courrier électronique est autorisée si les coordonnées du consommateur ont été recueillies directement auprès de lui, dans le respect des dispositions de*

*la loi n° 1.165 du 23 décembre 1993 , modifiée, à l'occasion d'une vente ou d'une prestation de services, si la prospection directe concerne des produits ou services analogues fournis par le même fournisseur, et si le consommateur se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé.*

*Dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le consommateur puisse utilement transmettre une demande*


*tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé ».*

**Les caméras dans les immeubles d'habitation**

Saisie à 2 reprises en 2022 la CCIN est intervenue :

- Concernant des caméras filmant les accès à la terrasse d'un particulier qui les avaient installées afin de s'assurer que personne n'entre chez lui par sa terrasse. Les riverains, craignant que ces caméras soient orientées vers leur logement, ont alerté la CCIN qui s'est assurée que tel n'était pas le cas.

- Pour demander de réorienter des caméras exploitées par 2 copropriétés qui filmaient respectivement la terrasse privative du plaignant, ainsi que les accès à sa terrasse. L'intervention rapide de la CCIN a permis de faire réorienter immédiatement les caméras en cause.

## L'exercice du droit d'accès indirect

En application de l'article 15 de la Loi n° 1.165, toute personne a le droit d'obtenir, de la part du responsable de traitement ou de son représentant, communication des informations la concernant sous forme écrite, non codée et conforme au contenu des enregistrements.

Cependant les informations contenues dans les traitements mis en œuvre par les Autorités judiciaires et administratives :

- intéressant la sécurité publique ;
- relatifs aux infractions, condamnations ou mesures de sûreté ;
- ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;

ne peuvent faire l'objet que d'un droit d'accès indirect qui s'exerce auprès de la CCIN.

L'article 15-1 de la Loi n° 1.165 précise que l'accès aux informations ne peut s'effectuer que par le Membre de la CCIN ayant la qualité de Magistrat du siège ou par le Commissaire nommé sur proposition du Conseil d'Etat, assisté par un Agent de la Commission dûment commissionné et assermenté à cet effet.

C'est dans ce cadre qu'au cours de l'année 2022 il a été procédé à l'exercice d'1 droit d'accès indirect, ayant pour origine un refus de délivrance d'un permis de travail en raison d'un avis défavorable émis par la Direction de la Sûreté Publique dans le cadre de l'enquête administrative préalable à la délivrance de ce document.

L'intervention de la CCIN a permis la mise à jour du dossier du plaignant, pour lequel plus aucune appréciation défavorable ne pourra être tirée des éléments à l'origine de l'avis défavorable initial.

## Les investigations

**Le traitement de données lié à la base Covid 19**

La CCIN a initié, fin 2022, une fois le pic de l'urgence sanitaire dépassé, une investigation afin de vérifier les modalités d'exploitation du traitement de données lié à la Base Covid, eu égard au nombre de personnes concernées et la nature sensible des informations qu'il contient.

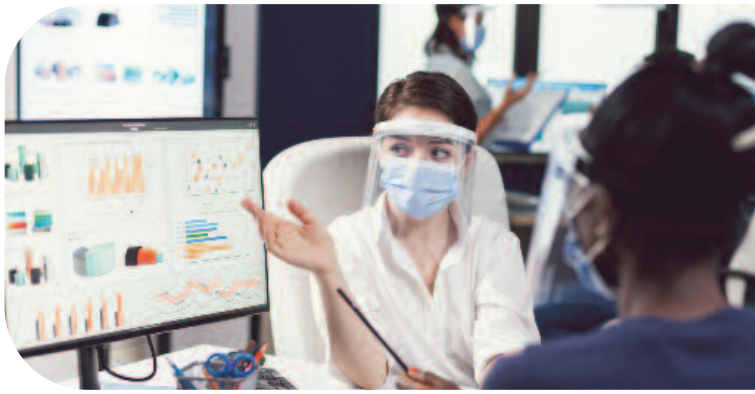
En application de l'article 18 de la Loi n° 1.165 du 23 décembre 1993, un médecin figurant sur la liste établie par le Conseil de l'Ordre des médecins de Monaco s'est joint à l'investigation lorsqu'il a fallu consulter des données médicales, auxquelles les personnels de la CCIN ne peuvent accéder.

Au cours de ce contrôle, différentes problématiques, potentiellement constitutives de non-conformités à la Loi n° 1.165, aux Décisions Ministérielles encadrant la création et l'évolution de la Base Covid et aux Avis de la Commission ont été relevées. Suite à cette investigation,

des modifications ont été apportées à la base Covid et sa sécurité a été renforcée.

Les manquements constatés et les corrections qui y ont été apportées par les Services de l'Etat permettront de repartir, si une situation similaire venait à se reproduire, sur une base plus protectrice des personnes concernées et de leurs données.

L'investigation devrait se clôturer en 2023.



**La mise à jour de la liste des membres d'une Association**

Une personne s'était préinscrite pour l'année 2021/2022 à une activité dans l'attente de sa réinscription définitive.

Cette préinscription avait été effectuée au travers d'une plateforme dédiée et précédait l'inscription définitive matérialisée par l'envoi d'un dossier papier et le règlement de frais d'inscription.

L'intéressé n'avait toutefois pas pu procéder à son inscription définitive et n'avait dès lors pas été en mesure de remplir le dossier d'inscription papier et de régler les frais d'inscription.

Un email lui notifiant la création de son compte d'adhérent pour l'année 2021/2022 lui avait pourtant été adressé. Ledit compte avait d'ailleurs fait l'objet de personnalisations en lien avec les préférences du plaignant.

Celui-ci a ainsi saisi la CCIN d'une plainte (voir supra Plaintes : Applications mobiles) pour l'utilisation potentiellement frauduleuse de certaines de ses données personnelles, en l'occurrence ses nom et prénom, sa date de naissance et son adresse email. Il était en outre possible que cette inscription « *de force* » eut été faite dans le but de pouvoir le sanctionner ensuite.

La Commission a décidé de faire procéder à une investigation sur place afin de vérifier notamment les moyens numériques mis en œuvre pour accéder au traitement des inscriptions afin de déterminer l'origine de l'inscription de l'intéressé ainsi que les logs de connexion relatifs à celle-ci.

L'investigation s'est déroulée sur le fondement de l'article 18-2 de la Loi n° 1.165 du 23 décembre 1993, soit, sur autorisation préalable du Président du Tribunal de Première Instance statuant sur Ordonnance sur requête, sans que les personnes investiguées puissent faire valoir leur droit d'opposition.

Lors des investigations, les agents ont constaté que l'inscription définitive des adhérents était effectuée sur la base d'un fichier Excel exporté au sein d'une application d'inscription. Une fois le tableau importé au sein de ladite application, l'inscription est validée et génère automatiquement un email informant la personne concernée de la création de son compte.

Il a été relevé l'existence d'une erreur entachant le tableau d'inscription relatif à la saison 2021/2022. Ce dernier contenait en plus des personnes inscrites pour la saison ceux inscrits au cours des années précédentes. Il n'y avait dès lors pas de volonté de nuire au plaignant.

Des mesures de corrections ont été apportées par le responsable de traitement dès l'issue des opérations de vérification afin de s'assurer que seules les personnes concernées soient intégrées au sein du listing des personnes définitivement inscrites et éligibles à la création d'un compte dédié.


# LES AVIS DE LA COMMISSION SUR LES PROJETS DE TEXTES LÉGISLATIFS ET RÉGLEMENTAIRES

La Loi n° 1.165 relative à la protection des informations nominatives prévoit en son article 2 dernier alinéa, que la CCIN est consultée par le Ministre d'Etat lors de l'élaboration de mesures législatives ou réglementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement des informations nominatives, et qu'elle peut l'être pour toute autre mesure susceptible d'affecter lesdits droits et libertés.

Dans ce cadre la Commission n'a été consultée en 2022 qu'à 2 reprises par le Ministre d'Etat, sur 2 projets de Décisions Ministérielles en lien avec la crise sanitaire, alors même qu'elle aurait dû l'être s'agissant notamment, sans que cette liste soit exhaustive, de l'élaboration :

- du projet de Loi modifiant la Loi n° 975 portant statut des fonctionnaires de l'Etat et du projet d'Ordonnance Souveraine portant dispositions générales de caractère statutaire applicables aux agents contractuels de l'Etat : si elle avait été consultée la CCIN n'aurait pas manqué d'appeler de ses vœux l'insertion de dispositions spécifiques prenant en compte la situation des fonctionnaires et des agents contractuels des Autorités Administratives Indépendantes, et d'émettre un avis sur les dispositions relatives à l'accès aux dossiers des personnes concernées, ainsi que sur les durées de conservation des données ;

- du projet d'Ordonnance Souveraine relative à la télémédecine, en ce que ce texte implique la collecte de données de santé, qui plus est par le biais de technologies de l'information et de la communication ;

- du projet d'Ordonnance Souveraine relative aux missions du Délégué à la prévention et à la lutte contre le harcèlement et la violence en milieu scolaire, en ce que ledit Délégué est en charge notamment de centraliser les signalements en la matière, sans que le texte encadre les durées de conservation des signalements, ainsi que les accès éventuels à ceux-ci ;

- du projet d'Ordonnance Souveraine portant application de l'article 34 de la Loi n° 1.383 pour une Principauté numérique, en ce que cette Ordonnance Souveraine prévoit des collectes et une conservation obligatoires de données par les personnes qui offrent des services de communication au public en ligne.

**Le projet de Décision Ministérielle modifiant la Décision Ministérielle du 1er juillet 2021 relative au passe sanitaire**

La CCIN a été saisie le 7 janvier 2022 en urgence pour donner son avis sur le projet de Décision Ministérielle modifiant la Décision Ministérielle du 1er juillet 2021 relative au passe sanitaire. Ce projet visait à étendre l'obligation de passe sanitaire.

A cette occasion, et suite à des échanges intervenus avec SEM le Ministre d'Etat, la Commission s'est interrogée sur le véhicule juridique choisi considérant notamment que s'agissant d'une mesure limitant la liberté du travail garantie par l'article 25 de la Constitution, une Loi était nécessaire et que le Règlement Sanitaire International sur lequel était basé ce projet de décision ministérielle n'était pas applicable en l'espèce dans la mesure où ce règlement régit les voyages internationaux et renvoie à la législation nationale pour le surplus des mesures sanitaires.

Elle s'est également interrogée sur le consentement des personnes concernées dès lors que ce projet visait à inciter fortement à la vaccination laquelle doit s'appliquer à des personnes qui y consentent aux termes de la Décision Ministérielle du 30 décembre 2020 et où ce consentement doit être libre et éclairé selon la Loi n° 1.454 du 30 octobre 2017.

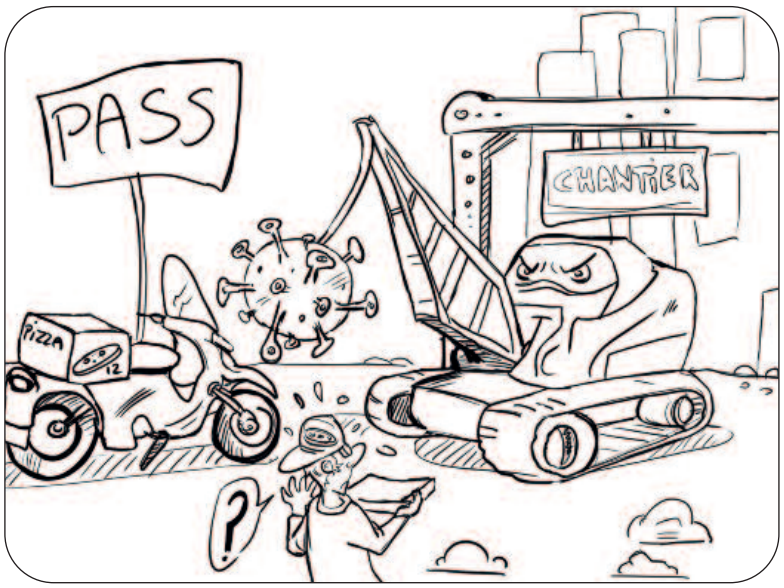
Elle s'est aussi émue du temps imparti pour obtenir ce passe sanitaire pour se rendre sur le lieu de travail et d'avoir eu connaissance que certaines entités avaient déjà mis en application le texte projeté. Elle a attiré l'attention des services sur le fait que l'application de mesures aussi impactantes ne pouvait être effective avant l'entrée en vigueur du texte les imposant, sauf à engager la responsabilité de l'employeur.

La Commission a pointé le problème des « *intervenants* » dans les établissements recevant des congrès, à défaut de définitions de ce statut et alors que l'assouplissement du passe sanitaire au moyen d'un test négatif ne leur semblait pas applicable, l'article des dérogations ne visant que les « *personnels* ».

S'agissant des personnes concernées, elle a mis en évidence une différence de traitement entre les établissements visés aux articles 7 et 8 comme par exemple les lieux de restauration et les chantiers concernant les interventions de personnes extérieures. Les intervenants ponctuels (livraison, architecte, ...) sur les chantiers devant, sauf urgence, présenter un passe sanitaire dès lors que le texte vise « *toute personne présente* » tandis que dans les autres établissements les livraisons sont exclues des personnes assujetties à cette obligation. Elle s'est questionnée sur la possibilité pour l'employeur de ces personnes extérieures au chantier de demander un passe sanitaire à leur salarié se rendant sur un chantier alors que leur métier n'est pas soumis à une telle obligation.

S'agissant des contrôles, outre ses remarques formulées dans sa délibération n° 2021-144 du 23 juin 2021 relative aux contrôles d'identité opérés par des personnes non habilitées et le véhicule juridique choisi pour ce faire, elle s'est interrogée sur leur mise en œuvre pratique.

En effet, le projet prévoyait que les responsables habilitent nommément les personnes autorisées à contrôler les justificatifs pour leur compte et tiennent un registre détaillant les personnes ainsi habilitées et la date de leur habilitation. Elle s'est donc interrogée sur le choix du Gouvernement et de la Mairie, lors de divers évènements, de déléguer le contrôle à une entreprise privée et sur la possibilité dans ces cas de connaître nommément les employés de leur prestataire et, le cas échéant, de leur faire endosser une responsabilité.




Concernant les personnes dont l'activité est indispensable pour la continuité d'activité de certaines entreprises, la Commission s'est interrogée sur la pertinence d'indiquer dans l'annexe les entités qualifiées d'OIV, cette qualité devant rester inconnue du public.

Elle a noté que le critère retenu était uniquement « *le caractère indispensable* » du travail de la personne pour la continuité d'activité de certaines entreprises ou de certains services publics « *assurant des services essentiels à la population* », notions non définies. Ce caractère indispensable devant être apprécié par les entités concernées sans en avoir les critères de mise en œuvre.

Après avoir évoqué quelques exemples de difficultés que pouvait poser ce point, elle a estimé que laisser ce pouvoir d'appréciation à l'employeur pouvait conduire à de graves disparités d'application, voire à des sanctions d'opportunité contre certains employés ou catégories d'employés, eu égard aux dispositions de l'article 9-2 qui emportent des conséquences financières importantes pour les personnes concernées par cette obligation de présentation d'un passe sanitaire. Elle a considéré qu'il conviendrait donc de préciser que cette obligation ne s'applique pas aux personnes effectuant l'intégralité de leur prestation à distance en application de la décision ministérielle du 30 décembre 2021 relative à l'adoption de conditions de travail à distance obligatoire pour les salariés, fonctionnaires ou agent de l'Etat et de la Commune, et pour tout ou partie de la durée hebdomadaire de travail.

Elle a estimé qu'il serait particulièrement opportun que la rédaction du projet d'alinéa 6 de l'article 9-1 soit modifiée afin de préciser que sont concernées par l'obligation de présentation d'un passe sanitaire les seules personnes dont l'activité concoure aux services essentiels à la population. En effet, au sein des entités listées en annexe, la totalité des salariés, fonctionnaires ou agents travaillant en leur sein ne concourent pas à des services essentiels à la population.

Suite à cet avis, SEM le Ministre d'Etat a opéré certaines des modifications suggérées dans sa décision définitive du 12 janvier 2022 publiée le 14 janvier 2022.

**Le projet de Décision Ministérielle modifiant la Décision Ministérielle du 20 mai 2020 relative à la mise en œuvre d'un traitement d'informations nominatives destiné à permettre le suivi épidémiologique prise en application de l'article 65 de l'Ordonnance Souveraine n° 6.387 du 9 mai 2017 relative à la mise en œuvre du règlement sanitaire international (2005) en vue de lutter contre la propagation internationale des maladies**

La CCIN a été saisie le 24 octobre 2022 par SEM le Ministre d'Etat d'une demande d'avis relative au projet de décision ministérielle modifiant la Décision Ministérielle du 20 mai 2020 relative à la mise en œuvre d'un traitement d'informations nominatives destiné à permettre le suivi épidémiologique prise en application de l'article 65 de l'Ordonnance Souveraine n° 6.387 du

9 mai 2017 relative à la mise en œuvre du règlement sanitaire international (2005) en vue de lutter contre la propagation internationale des maladies.

En préambule, la Commission a rappelé que l'article 6 de la Décision Ministérielle du 20 mai 2020 encadre les durées de conservation des informations contenues dans ledit traitement.

Le projet visait à modifier cet article avec pour conséquence d'allonger les durées de conservation des informations contenues dans la « *base Covid* » notamment en ce qui concerne l'anonymisation des données initialement prévue au 31 décembre 2022. Le Gouvernement considérait que cette anonymisation avait des conséquences négatives d'un point de vue médical.

La Commission a relevé que la Haute Autorité de Santé française avait établi différents scénarios épidémiologiques de vaccination à envisager dont il résultait que le statut d'infection au SARS-Cov-2 en France ne semblait pas être médicalement pertinent plus de 6 mois. Le décret du 12 mai 2020 disposait que les informations collectées étaient conservées six mois après leur collecte pour les données relatives à une personne ayant fait l'objet d'un dépistage virologique ou sérologique de la Covid 19 concluant à une contamination et trois mois après leur collecte pour les autres données.

Rappelant que les personnes concernées étaient suivies par leur médecin traitant, elle a réitéré ses inquiétudes quant à la conservation étendue d'informations médicales non pertinentes dans la base Covid qui sert à de multiples finalités aux intérêts de conservation différenciés. Elle a indiqué continuer à estimer qu'une durée de conservation/anonymisation fondée non pas sur la nature de l'opération en question (vaccination, test négatif, test positif) mais sur le fait que la personne ait ou non été vaccinée n'est pas opportune.

Elle a considéré que s'il était tout à fait fondé que la base Covid, pour certaines de ses finalités, voit sa durée d'exploitation étendue au-delà du 31 décembre 2022, tel n'était pas le cas de l'ensemble des informations qu'elle contient.

Elle a rappelé que cette base n'était pas actualisée, créant des disparités entre les personnes

figurant obligatoirement dans le traitement lors de la constitution initiale de la base Covid dont les informations ne sont jamais effacées et les nouvelles personnes éligibles à y être inscrites, qui peuvent choisir d'y échapper si elles ne se signalent pas en Principauté pour un test ou une vaccination.

Sur l'extension de la durée de conservation justifiée par le suivi médical, la Commission a relevé qu'en application du 2ème alinéa de l'article 6 en vigueur dont la suppression était envisagée, il ne devrait plus y avoir d'informations en lien avec le suivi médical datant de plus d'un an, sauf à ce que cette disposition n'ait pas été appliquée. Elle a constaté, au vu des dossiers qui lui ont été soumis, et notamment de l'étude CORDAGES qu'il était envisagé de traiter le suivi médical comme un dossier patient avec une rétention des informations bi-décennale.

Elle a rappelé qu'elle n'avait jamais été saisie du traitement du suivi médical pour en apprécier le fondement juridique et la proportionnalité. Elle a noté qu'en France, les informations ne pouvaient être conservées par l'Agence Régionale de Santé que 3 mois pour un suivi à domicile des malades et qu'aucun traitement mis en œuvre par l'Etat français ne lui permet l'exploitation d'un dossier médical qui serait propre à la gestion Covid, la CNIL et l'Assemblée Nationale ayant veillé à ce que les durées de conservation centralisées d'informations sensibles par l'Etat soient les plus courtes possibles.

La Commission a rappelé également avoir déjà demandé dans de précédentes délibérations à ce que la nature des informations renseignées au titre du suivi médical soient précisées dans la Décision Ministérielle du 20 mai 2020, ce qui n'a pas été fait.

Elle a estimé d'une part, qu'une durée de conservation courte des informations de santé est plus protectrice des droits et libertés fondamentaux des personnes concernées et d'autre part, qu'en application du 2ème alinéa de l'article 6 qu'il était projeté d'abroger, il aurait déjà dû être procédé à la suppression de nombreuses informations.

Concernant la référence à la Décision Ministérielle du 18 mai 2020, la Commission a noté qu'il n'y avait aucune explication sur le fait de lier le sort de l'anonymisation à la date d'abrogation de ladite Décision Ministérielle.

A titre liminaire, elle a relevé que la plupart des Décisions Ministérielles contenaient des mesures limitées dans le temps afin de minimiser les

atteintes aux droits et libertés fondamentaux qu'impose la gestion de la crise sanitaire. Elle a mis en exergue le fait que malheureusement, aucune Loi ni aucun texte n'encadre l'urgence liée à la crise sanitaire propre à la Covid 19, dont découleraient des délais applicables aux mesures exceptionnelles mises en œuvre par le Gouvernement et que jusqu'à présent, quand une date butoir d'une Décision Ministérielle est atteinte, une nouvelle Décision modificative vient en étendre la durée sans débat sur la pertinence et sur les équilibres en présence en termes de droit et libertés fondamentaux. Conséquence qui avait été anticipée par la Commission qui a maintes fois rappelé qu'un texte de nature législative devait encadrer la gestion de la crise.

En tout état de cause, considérant l'ensemble des points soulevés, et malgré les justifications avancées à leur appui, la Commission a estimé que les durées de conservation appliquées aux données exploitées dans la base Covid (hors vaccination) portaient une atteinte disproportionnée aux droits et libertés des personnes concernées.

Elle a regretté en outre que la crise sanitaire et le traitement d'informations nominatives qui en découle ne soient gérés que par le biais de Décisions Ministérielles, ce qui écarte tout débat pourtant nécessaire dans un Etat de droit. Elle a souligné à cet égard que les personnes concernées ne bénéficiaient pas de la prévisibilité ni d'un degré d'information suffisant sur le devenir des informations nominatives les concernant exploitées par l'Etat.

Dans sa Décision Ministérielle du 22 décembre 2022, publiée le 30 décembre 2022, SEM le Ministre d'Etat n'a pas modifié son projet initial malgré cet avis de la CCIN.

# 4

# LES TRAITEMENTS AUTOMATISES D'INFORMATIONS NOMINATIVES


## Le répertoire public des traitements

Le répertoire des traitements est un registre public destiné à assurer la publicité des traitements exploités par les personnes physiques et morales de droit privé, ainsi que par les entités publiques et assimilées.

Il peut être consulté au siège de la Commission par toute personne physique ou morale souhaitant s'assurer de l'existence légale d'un traitement automatisé d'informations nominatives.

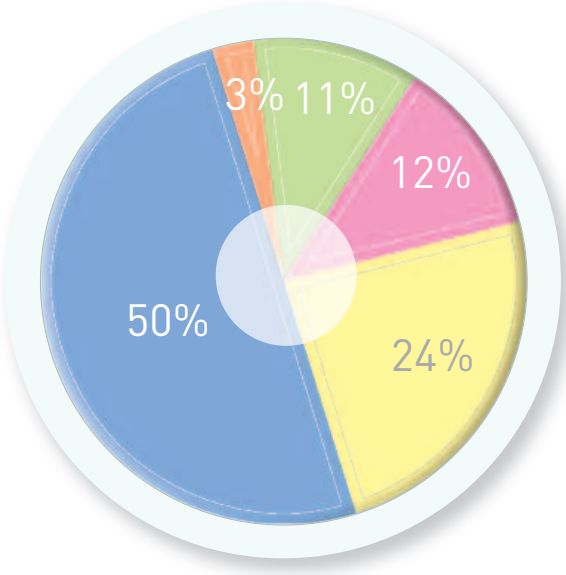

Seuls ne sont pas inscrits au répertoire public les traitements mis en œuvre par les Autorités Judiciaires et les Autorités Administratives qui concernent la sécurité publique, les infractions, les condamnations ou les mesures de sûreté, ou ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

**Nombre total de traitements inscrits au répertoire public au 31 décembre 2022 :**

**7.154** se répartissant ainsi :

- 785 traitements du secteur public ou assimilé ;
- 887 traitements ayant fait l'objet d'une autorisation de la Commission ;
- 1.714 traitements ayant fait l'objet d'une déclaration ordinaire ;
- 3.538 traitements ayant fait l'objet d'une déclaration simplifiée ;
- 230 autorisations de transfert vers un Pays ne disposant pas d'un niveau de protéction adéquat

**Traitements inscrits au répertoire public**



**Nombre de nouveaux traitements inscrits au répertoire en 2022 :**

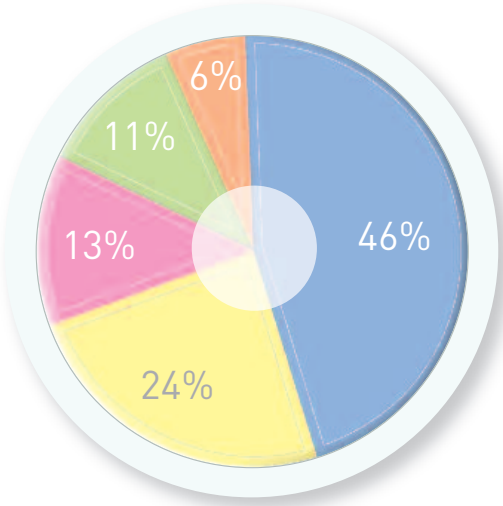
| Declaration simplifiée | Declaration ordinaire | Demande d'avis | Demande d'autorisation | Demande de transfert |
|---|---|---|---|---|
| 227 | 117 | 56 | 64 | 32 |

**Nombre total de traitements inscrits au répertoire en 2022**

**496** traitements ont été inscrits en 2022 au répertoire des traitements, se répartissant comme suit :

- **56** traitements ayant fait l'objet d'un avis favorable à leur mise en œuvre, relevant du secteur public ou assimilé ;
- **64** traitements dont la mise en œuvre a été autorisée par la Commission ;
- **117** traitements ayant fait l'objet d'une déclaration ordinaire ;
- **227** traitements ayant fait l'objet d'une déclaration simplifiée ;
- **32** autorisations de transfert de données vers un Pays ne disposant pas d'un niveau de protection adéquat.

Traitements inscrits en 2022




- Traitements ayant fait l'objet d'une déclaration simplifiée
- Traitements ayant fait l'objet d'une déclaration ordinaire
- Traitements ayant fait l'objet d'une autorisation
- Traitements du secteur public ou assimilé
- Autorisations de transfert vers un Pays ne disposant pas d'un niveau de protection adéquat

**Nombre de délibérations rendues par la Commission en 2022 :**

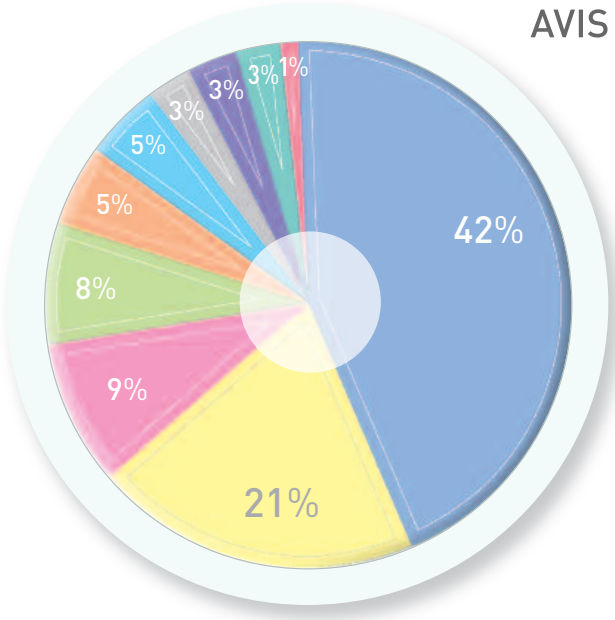
*Au cours de l'année écoulée, la Commission a rendu*

**186** délibérations se répartissant comme suit :

- **83** autorisant la mise en œuvre ou la modification de traitements
- **66** avis portant avis favorable à la mise en œuvre ou à la modification de traitements
- **32** autorisant un transfert d'informations nominatives vers un Pays ne disposant pas d'un niveau de protection adéquat
- **2** portant avis sur des projets de textes transmis par le Ministre d'Etat
- **3** portant sur une mission d'investigation

## Les traitements du secteur public

AVIS




- Etat de Monaco
- CHPG
- Commune
- Monaco Télécom
- Conseil National
- Services Judiciaires
- SMEG
- OPS
- CCSS
- Centre scientifique

**Une année sous le sceau d'une Administration Numérique**

Le développement du numérique en Principauté se traduit au niveau de la CCIN par la réception de plusieurs demandes d'avis transmises par le Gouvernement. Voici quelques exemples des traitements ayant reçu un avis favorable de la Commission.

Ainsi, a notamment été soumis en 2022 un traitement dont l'objectif « *est de permettre aux usagers de prendre rendez-vous avec le Service de l'Emploi et l'Inspection du Travail de la Direction du Travail* » en ligne.

En outre, la CCIN a eu à connaitre du traitement ayant pour finalité « *Gestion du compte permettant aux usagers d'entreprendre et suivre des démarches par téléservices* » et relatif au site dénommé « *MonGuichet.mc* », qui permet aux particuliers et aux entreprises de créer un compte leur permettant d'entreprendre et de suivre les démarches offertes par les différents téléservices qu'il crée. Ce traitement a pour vocation de remplacer le traitement ayant pour finalité « *Gestion du compte permettant aux usagers d'entreprendre des démarches par téléservices* ».

Par ailleurs, la Loi n° 1.482 a modifié la Loi n° 1.383 sur l'économie numérique, qui est ainsi devenue la Loi pour une Principauté Numérique. Celle-ci a introduit à Monaco, la notion de Service de confiance qui comprend la signature électronique et le cachet électronique. Les Organismes Publics doivent désormais accepter des documents signés électroniquement et peuvent en émettre.

Aussi, la Direction des Ressources Humaines et de la Formation de la Fonction Publique (DRHFFP) a été désignée comme Autorité d'Enregistrement afin de délivrer des Certificats qualifiés de signature et de cachet électroniques aux personnes dûment habilitées des Organismes du Secteur Public. Il est précisé que la DRHFFP pourra délivrer trois types de certificats aux personnes physiques représentant un organisme du secteur public: ceux permettant la signature électronique ; ceux qui pourront faire office de cachet et enfin, ceux permettant l'authentification. Le traitement dont s'agit a pour finalité « *Délivrance de Certificats qualifiés de signature et de cachet électroniques aux personnes dûment habilitées des Organismes du Secteur Public* ».

De plus, le traitement ayant pour finalité la « *Mise à disposition de la Direction des Travaux Publics d'une solution de Gestion Electronique Documentaire* » exploité par la Direction des Travaux Publics a été modifié pour permettre la gestion dématérialisée des appels d'offres, à savoir l'édition des appels d'offres et la création d'un espace de dépôt et d'échange entre la Direction des Travaux Publics et les différentes entreprises consultées.

Enfin, la Principauté a mis à disposition des monégasques et de ses résidents une identité numérique sur leurs cartes d'identité ou de résidents, dérivable sur mobile, et dont les traitements permettant sa

mise en œuvre ont reçu des avis favorables en 2021. Le Gouvernement a souhaité mettre à disposition de ces personnes un téléservice leur permettant de révoquer à tout moment et à distance leurs certificats si elles les estiment compromis, comme en cas de perte ou de vols de leurs cartes supports de leur identité numérique. Le traitement a pour finalité « *Permettre la création et la gestion d'un profil de révocation des certificats électroniques en ligne* » et est dénommé « *Profil de révocation MConnect* ».

**La gestion des flux de production des archives publiques et de leur consultation**

Par délibération n° 2022-184 du 21 décembre 2022, la CCIN a émis un avis favorable à la mise en œuvre d'un traitement opéré par la Mission de Préfiguration des Archives Nationales (MPAN) et le Service Central des Archives et de la Documentation Administrative (SCADA) suite à l'Ordonnance Souveraine n° 8.569 du 25 mars 2021 relative aux archives d'intérêt public.

La Commission a relevé que le logiciel permettait de consentir à la réception de newsletters et a rappelé qu'il devait en conséquence prévoir la possibilité de se désinscrire de cette réception.

Considérant que l'intitulé de ce traitement, « *Gestion d'archives d'intérêt public* », *n'était pas suffisamment explicite, elle l'a modifié en « Gestion du flux de production d'archives d'intérêt public et leur consultation* ».

Si elle a estimé que le traitement était licite et justifié par les textes législatifs et réglementaires, elle a rappelé qu'elle avait appelé de ses vœux, depuis plusieurs années, à un meilleur encadrement des archives publiques dès lors que celles-ci intègrent des informations nominatives et a regretté de ne pas avoir été consultée sur le projet de l'Ordonnance Souveraine susvisée, ce qui aurait permis d'éviter certaines difficultés que pose ce texte en la matière.

La Commission a noté que les informations nominatives collectées étaient très diverses et pouvaient contenir des données de santé, des informations faisant apparaître des appartenances politiques,

raciales, ethniques, religieuses, philosophiques ou syndicales, des données relatives aux mœurs, à la vie sexuelle ou aux mesures d'ordre social. Certains documents et les informations nominatives qu'ils contiennent pouvant être scannés, voire océrisés, et intégrés au logiciel et des informations nominatives portées dans des inventaires, que le document soit ou non numérisé. Sont également traitées des informations sur les personnes sollicitant l'accès à ces archives. Parmi ces dernières informations, figurent des informations relatives aux professeurs qui encadrent certains lecteurs et qui ne sont pas en lien avec les Services concernés.

Un espace « *commentaire* » étant prévu, elle a rappelé que celui-ci ne devait contenir que des informations objectives et non des données interdites ou des propos injurieux, la régularité de cette espace dépendant de la responsabilité du responsable de traitement.

Concernant l'information des personnes concernées, si elle est prévue sur le site du Gouvernement, elle ne s'adresse pas directement à celles-ci et ne peut se concevoir que pour les personnes dont les données sont transmises par les personnes produisant des archives d'intérêt public remises pour conservation au responsable de traitement mais ne peut valoir pour les personnes consultant des inventaires ou les archives ainsi que pour les personnes concernées par le traitement qui doivent bénéficier d'une modalité d'information directe et préalable. La Commission a donc considéré que cette modalité d'information n'était pas conforme aux dispositions de l'article 14 de la Loi n° 1.165 pour les personnes concernées. Elle a demandé à ce que la mention d'information précise que les informations nominatives contenues dans les archives d'intérêt public peuvent être communiquées dans le respect des dispositions légales aux personnes qui en font la demande.

Elle s'est inquiétée du fait que des données de santé puissent transiter et être conservées dans la messagerie et a sollicité l'utilisation d'un système sécurisé pour protéger ces données et toutes les données sensibles. Elle a également demandé la sécurisation des copies de documents d'identité.

Sur la durée de conservation, elle a distingué deux types de durée de conservation liés aux catégories de personnes concernées. Les données relatives aux personnes inscrites dans des documents passés en archives définitives à l'issue de leur durée d'utilisation administrative eu égard à leur intérêt historique, scientifique ou statistique qui sont conservées sans limitation de durée conformément à la réglementation et les données relatives aux utilisateurs de la solution ou aux lecteurs ainsi que l'historique des consultations d'archives. Concernant ces dernières, le responsable de traitement souhaitait les conserver sans limite de temps et 100 ans en ce qui concerne les informations relatives à la pièce d'identité de la personne qui consulte. Ces durées étant alléguées comme justifiées dans un intérêt historique et archivistique.

La Commission a cependant estimé qu'en dehors de ce qui s'apparentait à un registre des consultations, qui présente un intérêt archivistique, ces durées ne pouvaient être accordées concernant les données de traçabilité et d'horodatage du logiciel et a fixé leur durée de conservation à un an glissant sans extraction.

Elle a noté que les bordereaux de versement et d'élimination étaient conservés sans limitation de durée afin de constituer l'histoire des fonds d'archives et que les échanges entre les services et leurs utilisateurs publics et privés étaient conservés 10 ans afin d'assurer un suivi et pouvaient être conservés définitivement à des fins d'archives.

**La gestion du paiement des prestations et des aides sociales et la gestion des assistants familiaux et des tiers dignes de confiance par l'Office de Protection Sociale**

En janvier 2022, deux traitements mis en œuvre par l'Office de Protection Sociale (OPS) ont reçu un avis favorable de la Commission.

Le premier, « *Gestion du paiement des prestations et des aides sociales* », a pour objectif « *de permettre à l'Office de Protection Sociale, établissement public chargé du versement des aides sociales, administré par une Commission Administrative, d'exercer sa mission d'organisme payeur des prestations sociales décidées par l'Etat* ».

Le second, « *Gestion des assistants familiaux et des tiers dignes de confiance* » a pour objectif « *de permettre à l'Office de Protection Sociale (OPS), établissement public monégasque, d'accomplir sa mission de paiement des salariés et/ou indemnités aux assistants familiaux et tiers dignes de confiance, intervenant dans la protection des enfants accueillis, placés sur décision du juge tutélaire* ».

Pour ces deux traitements, le responsable de traitement a indiqué que « *Les opérations réalisées interviennent dans le prolongement d'une aide ou prestation sociale sollicitée par une personne, plus précisément dans sa phase de paiement ou de contentieux après paiement. Aussi, l'Office de Protection Sociale ne procède pas à l'information des personnes concernées conformément à l'exception prévue à l'article 14 alinéa 2 de la Loi n° 1.165 qui dispose que* : « *Lorsque les informations nominatives ne sont pas collectées directement auprès de la personne concernée, le responsable de traitement ou son représentant doit lui fournir les informations prévues au précédent alinéa, sauf si l'information de la personne concernée a déjà été effectuée, se révèle impossible, ou implique des mesures disproportionnées au regard de l'intérêt de la démarche ou encore si la collecte ou la communication des informations est expressément prévue par les dispositions législatives ou règlementaires* » ».

Le responsable de traitement a en outre précisé que « *l'Information des personnes concernées par les traitements de la Direction de l'Action Sanitaire et Sociale intègre dans les destinataires, l'OPS* ».

Si la Commission en a pris acte, elle a toutefois rappelé au responsable de traitement qu'il lui appartenait de s'assurer que les personnes concernées sont effectivement informées de la communication de leurs informations au sein du présent traitement.

La Commission a par ailleurs rappelé que les accès effectués aux informations métiers de la Direction de l'Action et de l'Aide Sociales par la Direction des Systèmes d'Information (DSI), ainsi qu'aux sauvegardes, doivent être tracés et conservés et a demandé qu'un message/une alerte soit envoyé(e) au responsable métier l'informant de cet accès qui sera préalablement justifié ou devra l'être.

De même, elle a demandé que toute réplication/copie des applications métiers et bases courriers soit autorisée par le responsable de Service, tracée par le système et fasse l'objet d'une alerte auprès du responsable métier.

En ce qui concerne la sécurité, la Commission a rappelé que toute communication d'informations confidentielles et/ou sensibles par voie électronique doit être sécurisée et que la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

Enfin, elle a demandé que les éléments de traçabilité des fiches bénéficiaires ne soient conservés qu'un an maximum.

**La « *Gestion de l'Allocation Parent Isolé* » et la « *Gestion de l'Allocation Parent au Foyer* » mises en œuvre par la Direction de l'Action et de l'Aide Sociales**

Deux nouvelles aides de l'Etat mises en œuvre par la Direction de l'Action et de l'Aide Sociales (DASO) ont fait l'objet d'un avis favorable de la Commission lors de la séance du 18 mai 2022.


La première, dénommée « *Allocation Parent Isolé* » ou « *API* » concerne « *toute personne veuve, divorcée, séparée ou abandonnée qui n'est pas mariée ou ne vit pas maritalement avec une autre personne et qui assume la charge effective et permanente d'un ou plusieurs enfants de nationalité monégasque* ».

La seconde, dénommée « *Allocation Parent au Foyer* » ou « *APF* », est octroyée à « *Toute personne, mariée ou vivant maritalement, ayant la charge effective et permanente d'un enfant de nationalité monégasque, âgé de moins de 12 ans ou de moins de 16 ans s'il est atteint d'un handicap l'empêchant de poursuivre une scolarité en milieu ordinaire et qui se consacre à son éducation* » à la condition « *qu'elle n'exerce aucune activité professionnelle, qu'elle ne soit titulaire d'aucun contrat d'apprentissage, ou qu'elle ne perçoive aucune rente, pension ou allocation issue d'une activité professionnelle présente ou passée* ».

Les deux avis de la Commission comportaient les mêmes remarques.

Elle a ainsi tout d'abord rappelé que les accès effectués aux informations métiers de la DASO par la DSI, ainsi qu'aux sauvegardes, doivent être tracés et conservés. La Commission a par ailleurs demandé qu'un message/une alerte soit envoyé(e) au responsable métier l'informant de cet accès qui sera préalablement justifié ou devra l'être.

De même, elle a demandé que toute réplication/copie des applications métiers et bases courriers soit autorisée par le responsable de service, tracée par le système et fasse l'objet d'une alerte auprès du responsable métier.

La Commission a également rappelé que toute communication d'informations confidentielles et/ou sensibles par voie électronique doit être sécurisée.

En outre, après avoir constaté que les informations et données sont enregistrées dans les fichiers Excel et Word sans sécurité, elle a demandé que

lesdites informations et données soient chiffrées ou ne soient uniquement accessibles que par les personnes ayant à en connaître.

Enfin, la Commission a demandé que les éléments de traçabilité ne soient conservés qu'un an maximum.

**Les traitements de la Direction des Services Judiciaires**

Si l'article 24-2-2° de la Loi n° 1.165 du 23 décembre 1993 exclut de son champ d'application « *les traitements mis en œuvre par l'autorité judiciaire pour les besoins des procédures diligentées devant les diverses juridictions ainsi que les procédures d'entraide judiciaire internationale* », cela ne concerne pas tous les traitements de la Direction des Services Judiciaires (DSJ). Aussi, la CCIN a été saisie, au cours de l'année 2022, de trois demandes d'avis sur des traitements d'informations nominatives mis en œuvre par cette entité.

La première saisine portait sur la mise en œuvre d'un traitement ayant pour finalité « *Gestion d'un coffre numérique permettant l'échange de documents entre les juridictions et les auxiliaires de justice* ». Par délibération du 16 mars 2022, la Commission a donné un avis favorable à sa mise en œuvre.

Le but de ce traitement est de permettre l'échange entre les Greffes, le Parquet Général et les Avocats-défenseurs, Avocats et Avocats-stagiaires des différentes pièces et messages afin de remplacer les anciens cartonniers physiques par une solution numérique sécurisée.

Ce traitement faisant l'objet d'un rapprochement avec le traitement « *ESABORA LEX* » qui était en cours de régularisation, il a été demandé à ce que celui-ci soit soumis dans les meilleurs délais à la Commission.

La deuxième saisine en date du 18 février 2022 était relative au traitement ayant pour finalité « *Gestion de la base courrier de la DSJ* ». Le but de ce traitement est la gestion des courriers émis et reçus par la

Direction des Services Judiciaires, le Secrétariat des ressources humaines du Palais de justice et de la Maison d'Arrêt et le regroupement des dossiers présentant un caractère sensible afin de permettre une bonne administration de la justice dans les différents domaines d'action de cette Direction. Un avis favorable à sa mise en œuvre a été donné.

Une interconnexion existant avec le traitement relatif au système d'authentification de la DSJ, il a été pris acte que ce dernier serait soumis à la Commission dans les plus brefs délais.

La troisième saisine en date du 11 avril 2022 concernait le traitement ayant pour finalité « *Gestion des étapes/liste/évènements permettant le suivi des procédures de l'ensemble des juridictions monégasques et édition du casier judiciaire* ». La Commission a également donné un avis favorable à la mise en œuvre de ce traitement destiné à la gestion de l'ensemble des procédures contentieuses et non contentieuses suivies devant toutes les juridictions et la tenue du casier judiciaire.

Relativement à l'information des personnes concernées, il a été noté que les personnels étaient informés par le biais de la Charte du système d'information de la DSJ publiée au Journal de Monaco et que dans certains cas, en fonction de la finalité des courriers et des réponses, une information des personnes extérieures concernées était effectuée.

La liste des destinataires auxquels des informations sont communiquées a été considérée comme justifiée.

Il a été relevé une interconnexion du traitement avec celui relatif à l'état civil légalement mis en œuvre et une prochaine interconnexion avec celui lié à la gestion des habilitations informatiques qui devra être soumis à la Commission dans les plus brefs délais.

**Les traitements mis en œuvre par le CHPG**

Le 20 avril 2022, la Commission s'est prononcée favorablement sur la mise en œuvre par le CHPG d'un traitement ayant pour finalité « *Gestion des données des joueurs de l'ASM dans le cadre de la détection et de la prise en charge des altérations neurocognitives liées à la pratique du football* ».

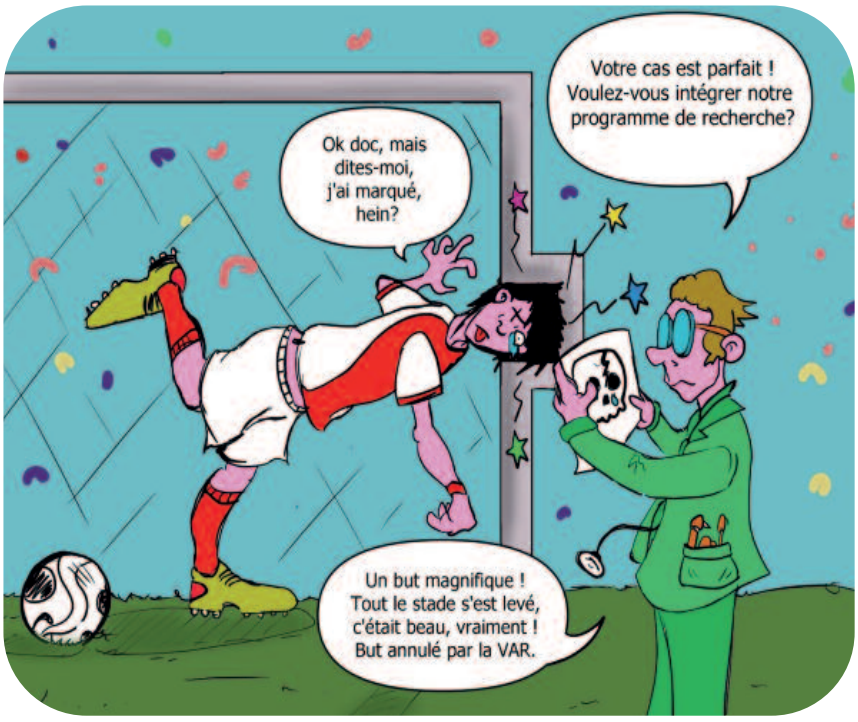
L'objectif de ce traitement « *est de constituer un Tableur qui regroupe l'ensemble des données pertinentes et essentielles à la détection, au suivi et à la prise en charge des altérations neurocognitives chez les joueurs de football de l'ASM* ».

Ces altérations neurocognitives pouvant être consécutives à des macro-traumatismes (commotions) ou à des microtraumatismes répétés (jeu de tête) survenant pendant la saison, ledit traitement s'inscrit ainsi dans une démarche de prévention qui est menée « *dans le cadre du suivi médical des joueurs, en soins courants* » et non pas dans le cadre d'une recherche médicale.

Le responsable de traitement a toutefois tenu à préciser qu' « *il n'est pas exclu, que dans le futur, une ou des études soient réalisées à partir de ces données. Mais dans ce cas un protocole d'étude sera rédigé, et si cette étude nécessite un traitement automatisé pseudo-anonymisé des données, il y aura une déclaration du traitement auprès de la CCIN* ».

Les informations collectées sont conservées 2 ans après la fin du contrat entre le joueur et l'ASM, à l'exception des logs de connexion qui sont conservés 1 an.

La Commission a cependant rappelé que l'information des personnes concernées doit impérativement être conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993 et a considéré qu'une procédure relative au droit d'accès par



voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Un mois plus tard, le 18 mai 2022, la Commission a également émis un avis favorable à la mise en œuvre du traitement ayant pour finalité « *Gestion du remplacement interne du CHPG* ».

Celui-ci a pour objectif de mener à bien la gestion des remplacements du personnel (uniquement en interne) par le biais d'une solution à laquelle tout personnel souhaitant postuler sur des missions temporairement vacantes peut s'inscrire.

La Commission a cependant demandé que le motif du remplacement qui figure déjà dans le traitement ayant pour fonctionnalité « *Gestion du temps de travail des personnels* », légalement mis en œuvre, ne soit pas collecté dans le présent traitement.

Par délibération n° 2022-158 en date du 16 novembre 2022, le traitement relatif à l'espace fitness mis en place par le CHPG afin d'améliorer la qualité de vie de son personnel au travail a reçu un avis favorable de la Commission sous réserve que l'information des personnes soit conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 et qu'une procédure relative au droit d'accès par voie électronique soit mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Enfin, lors de la dernière réunion de l'année, la Commission a prononcé 2 avis favorables supplémentaires, concernant les traitements ayant respectivement pour finalité « *Gestion des demandes de stage au CHPG* » et « *Gestion de la scolarité des étudiants en Institut de Formation en Soins Infirmiers et en Institut de Formation d'Aides-Soignants* ».

Là encore, elle a rappelé que l'information des personnes devait être conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 et considéré qu'une procédure relative au droit d'accès par voie électronique devait être mise en place afin de vérifier l'identité de la personne exerçant son droit d'accès.

La Commission a également demandé que les traitements ayant pour finalité « *Gestion des stages* » et « *Gestion des admissions à l'école des infirmiers et aides-soignants* », qui n'ont encore fait l'objet d'aucune formalité auprès d'elle, lui soient soumis dans les plus brefs délais.

**La protection des informations nominatives en matière de recherches dans le domaine de la santé**

Le Centre Hospitalier Princesse Grace (CHPG) a déposé en 2022, 7 demandes d'avis auprès de la Commission concernant des recherches médicales : un nombre en recul par rapport aux années précédentes.

*Les recherches biomédicales*

4 des 7 demandes déposées ont concerné des recherches biomédicales.

La première d'entre elles, dénommée « *CRI-RA* », a fait l'objet d'un avis favorable de la Commission le 16 février 2022.

Cet essai présenté par le Centre Hospitalier Universitaire de Bordeaux a pour objectif principal de comparer l'efficacité à 6 mois de l'association baricitinib-adalimumab au baricitinib seul sur la diminution de l'activité de la polyarthrite rhumatoïde (PR) chez des patients chez qui la réponse à une ou plusieurs biothérapies n'a pas été satisfaisante.

Il devrait concerner 178 patients au total dont 9 à Monaco suivis au sein du Service de rhumatologie du CHPG.

La délibération n° 2022-021 de la Commission contient néanmoins plusieurs observations.

Ainsi, après avoir noté que le mois de naissance des patients était collecté, elle a tenu à rappeler qu'aux

termes de l'article 10-1 de la Loi n° 1.165, il convient de limiter les informations collectées aux seules données nécessaires à la réalisation de la finalité du traitement.

En conséquence, tenant compte du faible nombre de patients inclus en Principauté, la Commission a demandé que le mois de naissance des patients soit supprimé du traitement si cette donnée n'est pas un impératif justifié par l'étude. Le mois de naissance pourra toutefois être conservé pour les personnes ayant 18 ans l'année de l'inclusion afin de permettre à l'investigateur de démontrer le respect des critères d'âge des personnes concernées.

La Commission a également demandé que le formulaire de consentement que signe chaque patient soit complété afin d'indiquer qu'en cas d'exercice du droit d'opposition au traitement des données, les informations collectées au préalable continueront à être utilisées dans le cadre de la recherche.


Enfin, elle a également rappelé que :

- si les nouvelles recherches portant sur les données collectées dans le cadre du présent traitement devaient impliquer des accès ou des communications non mentionnés dans la présente demande d'avis, une demande modificative devra lui être soumise ;
- si un transfert de données devait être effectué vers des destinataires non mentionnés dans la présente demande d'avis, ladite demande devra être modifiée ;
- si ce transfert devait s'effectuer vers un pays ne présentant pas un niveau de protection adéquat, une demande d'autorisation de transfert devra lui être soumise.

Lors de sa réunion en date du 19 octobre, la Commission a émis deux nouveaux avis favorables.

Le premier de ces avis concernait une étude multicentrique mise en œuvre par l'Etablissement Public de Santé de Ville Evrard, situé en France, qui a pour objectif principal d'évaluer l'efficacité de la rTMS (stimulation magnétique transcrânienne répétitive) réalisée en ouvert sur les symptômes de la dépression résistante en pratique courante entre la Baseline et la fin de la cure initiale (entre 4 et 6 semaines).

Cette recherche, dénommée « *DSNATUR* » devrait concerner 15 patients suivis au sein du Service de psychiatrie du CHPG.

Comme pour la recherche précédente, la Commission a demandé que le jour et le mois de naissance des patients soient supprimés du traitement si cette donnée n'est pas un impératif justifié par l'étude. Le mois de naissance pourra toutefois être conservé pour les personnes ayant 18 ans l'année de l'inclusion afin de permettre à l'investigateur de démontrer le respect des critères d'âge des personnes concernées.

Elle a également rappelé que si un médecin ou un ARC rejoignait la recherche après son début, l'identifiant et le mot de passe doivent lui être communiqués par deux canaux distincts.

Le second avis favorable a été émis pour l'étude « *NIRVANA-Lung* » présentée par UNICANCER qui doit concerner 6 patients atteints de cancer bronchique et suivis au sein du Service de radiothérapie du CHPG. Cette étude a pour objectif principal de comparer le taux de survie globale entre le traitement par anti PD-1 et chimiothérapie par rapport au traitement par anti PD-1 et chimiothérapie en association avec de la radiothérapie avec un rapport du taux à 1 an et 2 ans.

La Commission a demandé que le formulaire de consentement soit complété afin d'indiquer qu'en cas d'exercice du droit d'opposition au traitement des données, les informations collectées au préalable pourraient continuer à être utilisées dans le cadre de la recherche.

Elle a par ailleurs formulé plusieurs remarques concernant la sécurité du traitement, à savoir que :

- les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises ;
- la communication sécurisée des données pseudonymisées et des mots de passe doit être effectuée par deux canaux distincts ;
- si un médecin ou un ARC rejoignait la recherche après son début, l'identifiant et le mot de passe doivent lui être communiqués par deux canaux distincts.

Enfin, lors de sa réunion du 21 décembre 2022, la Commission s'est prononcée favorablement à la mise en œuvre par le Centre Hospitalier Universitaire de Montpellier de l'étude « *SEQUENS-RA* », dont l'objectif principal est de comparer le pourcentage de rémission (DAS28-CRP↓2.6) obtenu durant les 9 mois après la randomisation, avec la stratégie thérapeutique séquentielle utilisant l'abatacept,

contre la stratégie de routine utilisant des anti-TNF (TNFi), chez les patients ACPA positif répondant à une premier TNFi, initiée trois mois avant la randomisation.

5 patients suivis au sein du Service de rhumatologie du CHPG devraient être inclus dans cette recherche.

Si la Commission s'est félicitée que la conservation des prélèvements à l'issue de la recherche au sein d'une collection d'échantillons biologiques à d'autres fins de recherche (dont génétique) dans le domaine des maladies rhumatoïdes fasse l'objet d'un consentement séparé par le biais de deux cases à cocher au sein du formulaire de consentement, afin que le patient puisse effectivement y consentir ou s'y opposer, elle a toutefois rappelé que si ces nouvelles recherches devaient impliquer des accès ou des communications non mentionnés dans la présente demande d'avis, ladite demande devra être modifiée.

Par ailleurs, après avoir relevé à la lecture du document d'information que les données pourraient être communiquées vers des personnes, sociétés et agences pouvant être situées « *dans d'autres pays de l'UE et de l'Espace Economique Européen (EEE), aux Etats-Unis et dans d'autres pays à l'extérieurs de l'UE et de l'EEE* » et qu' « *Il est possible que certains pays hors de l'UE et de l'EEE n'offrent pas le même niveau de protection de la vie privée* », la Commission a rappelé que si un transfert de données devait être effectué vers des destinataires non mentionnés dans la présente demande d'avis, ladite demande devra être modifiée.

De même, si ce transfert devait s'effectuer vers un pays ne présentant pas un niveau de protection adéquat, une demande de transfert devra lui être soumise.

Enfin, comme souvent, la Commission a rappelé que si un médecin ou un ARC rejoignait la recherche après son début, l'identifiant et le mot de passe doivent lui être communiqués par deux canaux distincts.

*Les recherches non biomédicales*

Parallèlement à ces 4 recherches, la Commission a eu à connaitre de 3 études non biomédicales.

C'est ainsi que le 19 janvier 2022, elle a émis un avis favorable à la recherche observationnelle présentée par le Centre Hospitalier Universitaire de Clermont-Ferrand. Dénommée « *eDOL* », celle-ci a pour objectif principal, chez les patients suivis dans les Structures Douleur Chronique pour le traitement d'une douleur chronique, de réaliser une analyse exploratoire multimodale des déterminants et des retentissements de la douleur chronique, et de leur évolution dans un contexte de vie réelle, en prenant en compte tous les évènements environnementaux susceptibles d'influencer la douleur chronique (traitements, antécédents, comorbidités...).

En Principauté de Monaco, cette recherche sera réalisée au CHPG sous la responsabilité d'un médecin investigateur exerçant au sein du Service Algologie. 5000 patients sont concernés au total dont environ 200 à 250 à Monaco.

La Commission a toutefois noté que dans le cadre de ce traitement des données statistiques (cookies) étaient collectées. Elle a donc demandé au responsable de traitement de s'assurer que les personnes concernées soient préalablement informées du dépôt et du destinataire desdites données afin de les accepter ou de les refuser.

Par délibération n° 2022-034 du 16 mars 2022, la Commission s'est également prononcée favorablement à la mise en œuvre par le CHPG de l' « *Etude NATURE* », une étude observationnelle monocentrique ayant pour objectifs d'évaluer l'efficacité et la tolérance du traitement de la


névralgie du trijumeau par radiochirurgie et de constituer une base de données des patients traités par radiochirurgie pour une névralgie du trijumeau.

Environ 30 patients suivis dans le Service de radiothérapie du CHPG devraient être concernés chaque année.

L'information préalable de ces patients a toutefois fait l'objet de deux demandes de la Commission, à savoir que la « *Note d'information* » soit complétée afin d'une part d'indiquer que les données déjà collectées ne pourront pas être effacées afin de sauvegarder l'intégrité scientifique de l'étude et d'autre part de préciser que le droit d'accès auprès du médecin référent s'exerce par voie postale ou sur place.

Le 20 avril 2022, l'« *Etude KONTINUE* » présentée par le CHPG a également reçu un avis favorable de la Commission.

Cette recherche observationnelle monocentrique prospective qui doit concerner 80 patients suivis dans le Service d'Algologie du CHPG, a pour objectif principal d'évaluer l'efficacité à long terme d'une perfusion continue de faibles doses de kétamine pendant 4 jours associée à du sulfate de magnésium chez les patients douloureux chroniques et pour objectif secondaire d'analyser les variables correspondant au soulagement des patients répondeurs et identifier les liens de causalité.

Elle n'a fait l'objet d'aucune remarque particulière de la part de la Commission.

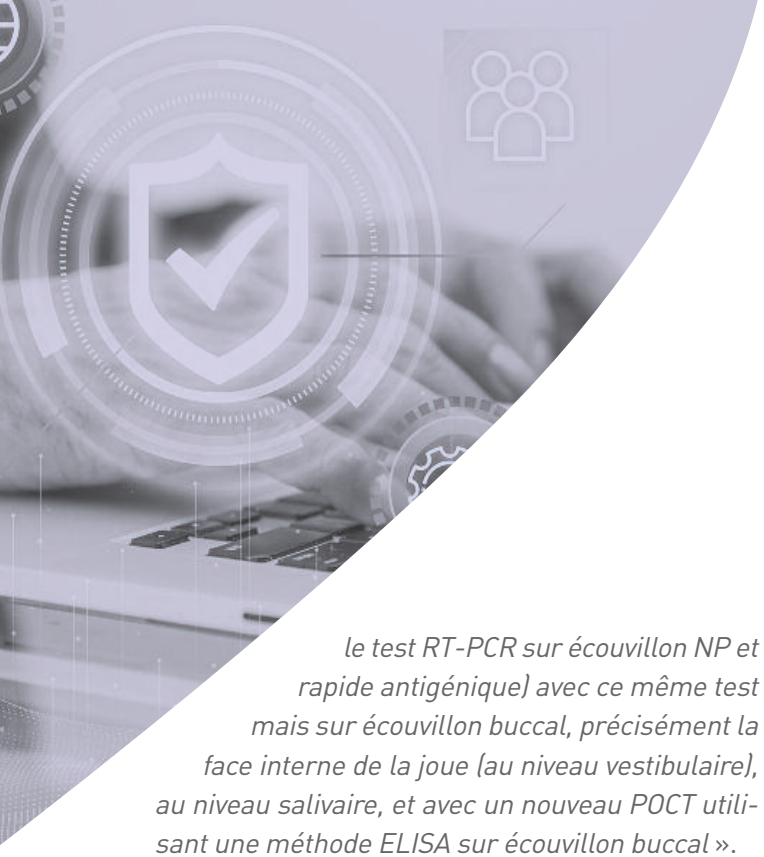
***L'étude Cordages exploitée par la Direction de l'Action Sanitaire***

Par délibération du 22 juin 2022, la Commission a émis un avis favorable, avec réserves, au traitement ayant pour finalité « *Etude permettant d'évaluer selon les antécédents médicaux des patients l'efficacité et la précision des différents modes de dépistage du virus Sars-CoV-2* ».

Il concerne principalement les patients qui acceptent de participer à l'étude lorsqu'ils se rendent à un centre de dépistage public pour suspicion clinique de COVID19 ou après contact avec un cas confirmé. Il y est précisé que « *Les participants sont inclus s'ils sont âgés de 18 ans ou plus et s'ils ont la capacité de fournir un consentement écrit, en excluant les individus faisant partie d'un dépistage préventif pour les groupes professionnels, et ceux ne pouvant s'engager à revenir dans les 48-72 heures suivant la première visite* ».

Le responsable de traitement a indiqué que « *L'objectif de l'étude Cordages est d'offrir plus de chances de détecter le virus du SARS-CoV-2. Lors d'un dépistage du virus réalisé par un test RT-PCR et rapide antigénique, il est proposé au patient de participer à l'étude en réalisant un prélèvement supplémentaire (salivaire et buccal). Si le patient accepte de participer à l'étude, ce dernier va devoir répondre à des questions sur son état de santé permettant de préciser les résultats obtenus* ».

Le responsable de traitement a expliqué que « *cette étude prospective comparera la précision diagnostique entre test de référence (c'est-à-dire*



*le test RT-PCR sur écouvillon NP et rapide antigénique) avec ce même test mais sur écouvillon buccal, précisément la face interne de la joue (au niveau vestibulaire), au niveau salivaire, et avec un nouveau POCT utilisant une méthode ELISA sur écouvillon buccal* ».

Il a en outre précisé que les objectifs secondaires sont :

- « *Évaluer la précision diagnostique de la RT-PCR et rapide antigénique et du POCT sur prélèvement buccal et salivaire par rapport aux valeurs d'amplification quantitative (Ct) du test RT-PCR sur écouvillon NP ;*
- *Analyser les seuils de cycle d'amplification de test RT-PCR (Ct) et rapide antigénique et la précision diagnostique du POCT en fonction de la présence et de la date des symptômes ;*
- *Parmi les participants symptomatiques, comparer les présentations cliniques entre les participants positifs et négatifs au test RT-PCR et rapide antigénique sur écouvillon NP.*

*Le test RT-PCR et rapide antigénique peut être d'une sensibilité imparfaite. En utilisant un modèle de classe latente bayésienne, nous évaluerons la vraie précision du POCT, car il ne nécessite pas de supposer qu'un test ou une combinaison de tests sont parfaits* ».

Lors de l'examen du dossier, la Commission a dû se questionner quant à la conservation des informations objets de l'étude au sein du traitement ayant pour finalité « *Prise en charge des patients dans le cadre du virus SARS-CoV-2* » ;

La Commission a relevé que l'article 10 de l'Ordonnance Souveraine n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé dispose que « *Lorsqu'un médecin-inspecteur, un médecin du travail, un médecin conseil d'un organisme de sécurité sociale ou un médecin contrôleur d'un assureur loi pratique ou fait pratiquer, en application de dispositions légales ou réglementaires, un ou plusieurs examens médicaux sur une personne, il tient, pour celle-ci, un dossier médical soumis aux dispositions des articles 11 et 12 et à celles des premier et quatrième alinéas de l'article 13 et contenant l'ensemble des données de santé à caractère personnel de cette personne, produites et reçues dans le cadre de ces examens* », et donc qu'il n'avait pas vocation à s'appliquer à l'étude « *Cordages* ». En effet, les personnes qui participent sur la base du consentement à une étude sont hors des cas d'une « *application de dispositions*

*légales ou règlementaires* », relativement à des « *examens médicaux* » qui en l'espèce (tests de dépistage Covid) ne sauraient à eux seuls justifier de la collecte de tels antécédents médicaux (tabagisme, cancer, diabète). Il convient en outre de constater que l'étude concernait des personnes qui ne nécessitent pas a priori d'accompagnement médical pour des complications en lien avec la COVID19.

La Commission avait en outre, en l'absence de formalité légale dédiée au dossier patient dont il était question, peu de certitudes sur le régime juridique applicable à celui-ci.

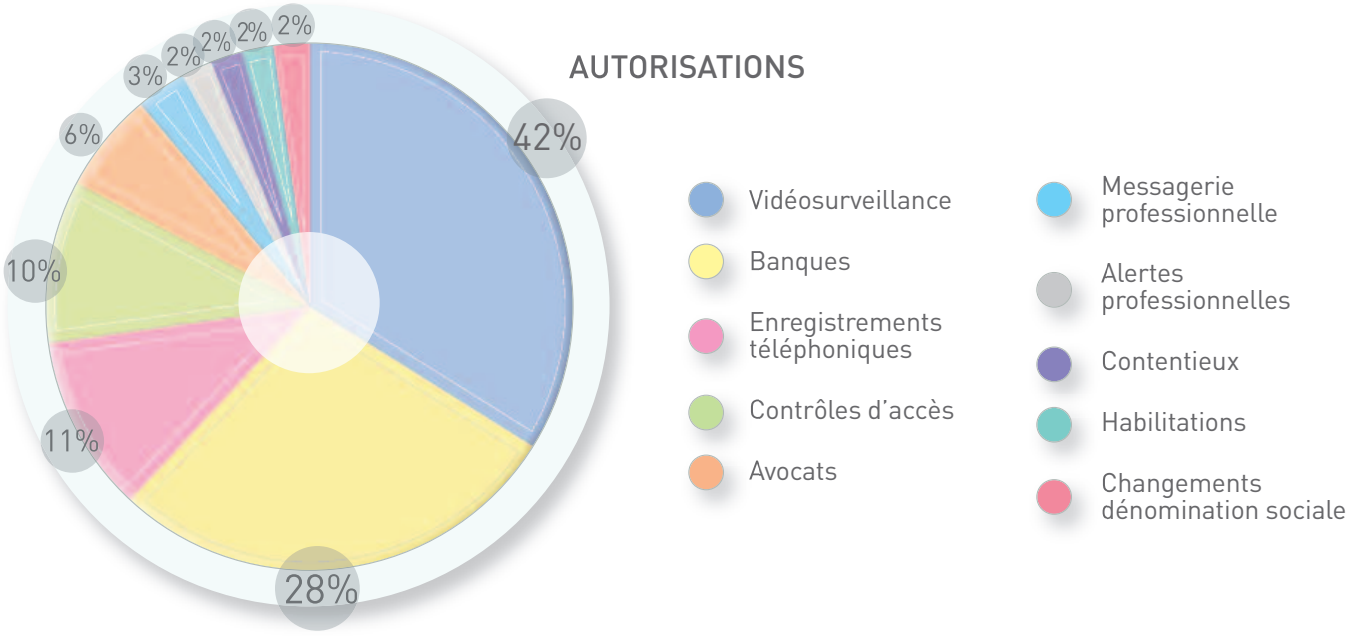
Elle a de plus relevé que cette dichotomie entre une conservation des données dans le traitement du suivi patient et une anonymisation de ces mêmes données dans le cadre de l'étude Cordages n'était pas expliquée au sein des mentions d'information des personnes concernées. Aussi, ces dernières pouvaient percevoir certaines contradictions qui ne leur permettaient pas de comprendre ce qu'il advient précisément de leurs informations médicales.

La Commission avait dès lors estimé que les antécédents médicaux des personnes concernées ne devraient pas figurer dès l'origine dans leur dossier médical et avait demandé au responsable de traitement de lui revenir dans les meilleurs délais pour justifier de la nécessité éventuelle d'une telle conservation et, le cas échéant, des moyens techniques mis en œuvre pour isoler et sécuriser les informations des sujets de l'étude.

Elle avait également constaté que les informations sont dans tous les cas conservées 20 ans dans, ou en lien, avec le dossier patient (questionnaire Cordages et formulaires de consentement), mais a demandé que le dossier patient ne soit pas alimenté par ces informations en l'absence d'éléments justifiant la nécessité de leur conservation pour mener à bien l'étude. La Commission avait indiqué qu'elle réétudierait la durée de conservation des informations avec les informations complémentaires, le cas échéant, du responsable de traitement.

Faisant suite à la délibération, le responsable de traitement a indiqué par courrier que le dossier patient ne sera plus alimenté par les informations en lien avec l'étude « *Cordages* », et que leur accès sera strictement limité aux médecins en charge de l'étude.

## Les traitements du secteur privé : focus sur des problématiques spécifiques



**La prévention des fuites de données**

La Commission s'est prononcée, lors de différentes séances plénières, sur la mise en œuvre, par des établissements bancaires, de traitements relatifs à la prévention des fuites de données aussi connus sous le nom DLP pour « *Data Leak Prevention* ».

Afin d'éviter la fuite de données confidentielles, les organismes se dotent d'outils et/ou mettent en œuvres différentes politiques permettant d'abord d'identifier, ensuite de contrôler et enfin de protéger les informations.

Les demandes soumises à la Commission ont porté essentiellement sur l'analyse des flux Internet des collaborateurs. Cependant, des outils DLP peuvent être déployés sur différents canaux de communication, notamment l'utilisation de la messagerie professionnelle ou encore l'utilisation de la messagerie instantanée.

Le déploiement d'un outil DLP peut d'abord se justifier par l'existence d'un intérêt légitime du responsable de traitement à protéger les informations relatives à son activité et aux clients.

La mise en place d'un tel outil peut également être justifiée par l'existence d'une obligation légale à laquelle il est soumis, notamment en application de l'article 270-3 de l'Arrêté français du 3 novembre 2014, relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution, qui dispose que « *les entreprises assujetties établissent par écrit une politique de sécurité du système d'information qui détermine les principes mis en œuvre pour protéger la confidentialité, l'intégrité et la disponibilité de leurs informations et des données de leurs clients, de leurs actifs et services informatiques. (...) En application de leur politique de sécurité du système d'information, les entreprises assujetties formalisent et mettent en œuvre des mesures de sécurité physique et logique adaptées à la sensibilité des locaux, des actifs et services informatiques, ainsi que des données* ».

Ce type de traitement étant mis en œuvre à des fins de surveillance, la Commission rappelle systématiquement que la finalité doit être limitée à la prévention des fuites de données et ne doit pas conduire à une surveillance permanente et inopportune des salariés.

Dans le cadre de l'instruction de ce type de dossier, la Commission est particulièrement attentive à la qualité

de l'information fournie aux personnes concernées pour apprécier la proportionnalité du traitement. A cette fin, la mention d'information doit :

- être adaptée et propre à chacun des outils mis à leur disposition, et
- reprendre l'ensemble des informations listées à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Afin de remplir son obligation d'information préalable des collaborateurs, le responsable de traitement peut notamment mettre à la disposition de ces derniers :

- un règlement intérieur ;
- une charte informatique ;
- un email de sensibilisation ;
- des documents dédiés.

L'objectif d'une information préalable adaptée et complète est de permettre aux collaborateurs de savoir quels sont les comportements attendus dans l'utilisation des différents outils mis à leur disposition et ainsi adapter leurs actions.

Les outils DLP pouvant lire les flux des sites internet consultés par les salariés, ils peuvent théoriquement permettre au responsable de traitement de connaître les informations de type messagerie privée (si l'utilisation est autorisée par le responsable de traitement) ou encore les informations relatives aux paiements par carte bancaire. Aussi, l'information fournie aux salariés ne peut être générique et doit donc être adaptée à chaque outil mis à leur disposition.

Enfin, la Commission rappelle également que ce type de traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993. Dès lors, si l'outil DLP a détecté une potentielle fuite de données et qu'une alerte a été générée, celle-ci ne peut directement donner


lieu à des sanctions ou autres mesures, à l'encontre du salarié concerné, sans qu'il n'y ait au préalable une intervention humaine pour analyser l'incident et ainsi différencier les fausses alertes de celles qui révèlent une tentative de fuite de données.

**Les appels téléphoniques de clients mystères dans un but de vérification de la qualité des prestations du service clientèle**

La CCIN a été saisie le 5 avril 2022 par une société de service d'une demande d'autorisation de traitement ayant pour finalité « *Evaluer la qualité de la prestation de réservation téléphonique des collaborateurs de la société par la réalisation d'appels mystères* ».

L'objectif de ce traitement était d'améliorer la qualité du traitement des appels clients réservant une prestation réalisée en langue française ou anglaise. Il était mis en œuvre avec le concours d'un prestataire extérieur à la société.

S'agissant de la licéité et de la justification du traitement, la Commission a considéré que ces critères étaient remplis dès lors que la mise en place était effectuée dans un objectif de formation et de contrôle qualité exclusivement et qu'il consistait en quelques appels mensuels aléatoires en sorte qu'il ne conduisait pas à une surveillance permanente et inopportune des salariés. Ce dernier point est vérifié de manière systématique par la Commission dès lors que des traitements sont amenés à surveiller le travail du salarié et/ou son temps de travail, un juste équilibre devant être ménagé entre le but du traitement, sa finalité dans l'intérêt légitime du responsable de traitement et les droits et libertés fondamentaux des personnes concernées.

Cependant, à la lecture de la grille d'évaluation jointe au dossier, elle a appelé l'attention du responsable de traitement sur la nécessité de définir des critères purement objectifs d'évaluation et sur la nature des commentaires et des attentes qui seront inscrits dans la partie de la grille relative au comportement du salarié.

Le responsable de traitement a par ailleurs indiqué que les informations collectées étaient conservées le temps de la durée d'embauche, excepté les communications téléphoniques qui étaient supprimées deux mois après leur collecte et les grilles d'évaluation qui étaient supprimées 24 mois après afin de pouvoir suivre chez les personnes concernées les axes d'amélioration identifiés.

A cet égard, la Commission a rappelé que cette durée de conservation s'appliquait quel que soit le support de sauvegarde des informations et s'est inquiétée que les rapports soient conservés plus longtemps dans la messagerie professionnelle des managers.

Aussi, elle a estimé que ces derniers ne devraient pas se voir communiquer le rapport par mail mais

devraient être simplement informés par ce moyen qu'un rapport est disponible sur leur espace de gestion en ligne.

**La dématérialisation des bulletins de paie et autres documents RH**

La CCIN a été saisie pour avis, par une société concessionnaire de service public, concernant la mise en œuvre d'un traitement ayant pour finalité « *Gestion de la dématérialisation des bulletins de paie et autres documents RH* » afin de proposer aux salariés des bulletins de paie et autres documents concernant la gestion des ressources humaines sous format électronique via notamment deux coffres-forts un pour les salariés, chacun d'eux disposant en son sein d'un coffre-fort individuel et personnel et l'autre pour l'employeur.

Cette dématérialisation est prévue depuis la modification de la Loi n° 638 du 11 janvier 1958 intervenue le 17 décembre 2019 et l'Arrêté Ministériel n° 2019-1088 du 20 décembre 2019 qui réglementent la délivrance des bulletins de paie sous forme électronique, sauf opposition du salarié qui peut demander à conserver une version papier de ce document.

La Commission a estimé que l'intérêt légitime était justifié par la volonté du responsable de traitement de simplifier les démarches et de mettre à disposition des salariés des coffres-forts numériques assurant la rapidité, la fiabilité, la sécurité et la disponibilité des documents.

Il est à noter que le responsable de traitement a prévu le recours à un prestataire extérieur mais également à un tiers séquestre de ce fournisseur afin de conserver la clé de chiffrement en cas de disparition du fournisseur, assurant ainsi une sécurité supplémentaire pour garantir la pérennité de l'accessibilité des documents.

Concernant la durée de conservation des informations, la Commission a fixé la durée minimum de conservation des bulletins de paie à 5 ans à compter de leur émission en application des dispositions de l'article 6 de l'Arrêté Ministériel n° 2019-1088 susvisé qui impose une telle durée de conservation alors que l'employeur souhaitait une conservation le temps de la relation contractuelle augmentée d'un mois. En revanche, concernant les informations temporelles, elle a réduit la durée de conservation initialement prévue le temps de la relation contractuelle augmentée d'un mois pour la fixer à 3 ans glissants compte tenu de la nature spécifique des documents concernés.

Sous ces conditions, elle a émis un avis favorable à la mise en œuvre de ce traitement.

# 5

# LA CCIN SUR LE TERRAIN

Afin de connaître les attentes, les projets, les interrogations des responsables de traitement, sur la protection des informations nominatives, les Agents de la CCIN se tiennent à l'écoute des acteurs économiques et publics.

La CCIN participe fréquemment à des événements dédiés à la protection des données afin d'échanger avec ses homologues, ainsi qu'avec des spécialistes de la matière.

**Intervention à un atelier sur les données personnelles au sein des organisations internationales**

La CCIN a été invitée, en tant que Vice-Présidente du Groupe de Travail sur le Rôle de la Protection des Données Personnelles dans l'Aide Internationale au Développement, l'Aide Internationale Humanitaire et la Gestion de Crise (GT AID), à participer en tant qu'intervenant à l'atelier « *les Données personnelles au sein des organisations internationale*s » organisé par le Contrôleur européen de la protection des données (CEPD ou EDPS en anglais) et le Programme alimentaire mondial (WFP) les 12 et 13 mai 2022 à Rome.

Réunissant une centaine de participants, cet évènement, créé en 2015, a permis à une cinquantaine d'organisations internationales de dialoguer sur les problèmes qu'elles peuvent rencontrer lors du traitement de données personnelles dans le cadre de leurs activités et de partager des informations et bonnes pratiques en matière de confidentialité et de respect de la vie privée.

Lors d'un panel dédié aux derniers développements en matière de protection des données, la CCIN a ainsi eu l'occasion de présenter le GT AID qui a été établi en 2020 par l'Assemblée mondiale pour la vie privée, ainsi que les actions que ce

groupe de travail a déjà menées au cours de sa première année d'existence, à savoir l'établissement d'une cartographie géographique et thématique des acteurs pertinents en matière d'aide au développement et d'aide humanitaire et l'élaboration d'un questionnaire sur les pratiques en matière de protection des données personnelles de ces acteurs dans la mise en œuvre de leurs programmes et projets.

**Conférence internationale « *Computers, Privacy and Data Protection* »**

La CCIN a assisté par l'intermédiaire de deux de ses agents à l'Edition 2022 de la Conférence internationale « *Computers, Privacy and Data Protection* » (CPDP) qui s'est tenue à Bruxelles du 24 au 26 mai 2022.

Cette Conférence annuelle rassemble des acteurs de haut niveau de la sphère internationale de la protection des données autour de discussions et de débats portant sur des sujets majeurs et actuels en lien avec la protection des données.

L'Edition 2022 a principalement axé son panel autour de thèmes relatifs au transfert de données, à la régulation des flux mondiaux ainsi qu'à la gouvernance et la réglementation de l'Intelligence Artificielle (IA).

Le transfert de données personnelles demeure un sujet majeur. Les intervenants ont à cet effet abordé les enjeux liés à ces transferts à la lumière d'une approche comparative des législations et autres textes en la matière. En effet, dans la foulée de l'adoption en Europe du Règlement Général sur la Protection des Données (RGPD) de nombreux pays, tels que récemment le Brésil et la Chine, se sont dotés de dispositions visant à régir la protection des données et encadrer les transferts de données. Cet encadrement a plus particulièrement été discuté par de nombreux panellistes à l'aune des arrêts SCHREMS I et II lesquels ont invalidé les cadres juridiques (Safe Harbor et Privacy Schields) qui servaient jusqu'alors de support aux acteurs européens (UE et EEE) pour les transferts de données opérés vers les Etats-Unis.

La question de la « *surveillance* », entendue comme l'accès par des Gouvernements aux données transférées, a également été évoquée au cours de ces échanges.

De nombreuses conférences ont par ailleurs abordé la problématique de l'IA et plus particulièrement sa gouvernance, sa réglementation et ses impacts en termes de protection des données et des droits fondamentaux alors qu'au niveau européen l'AI Act est encore à l'état de projet après qu'une proposition initiale ait été publiée au cours du premier semestre de l'année 2021. L'ensemble des instruments transversaux plus ou moins contraignants existants à l'heure actuelle (Principes de l'OCDE, Lignes directrices du G20, Recommandation de l'UNESCO sur l'éthique de l'IA, travaux du Conseil de l'Europe) a également été passé en revue.

De même, les liens entre IA et reconnaissance faciale ainsi que les risques de menace pour la vie privée des personnes ont également été évoqués au travers d'un état des lieux dans le monde.

**La CCIN présente au Forum International de la Cybersécurité 2022 devenu le « *Incyber Forum* »**

La CCIN était présente à la 13ème édition du Forum International de la Cybersécurité (FIC) 2022 du 7 au 9 Juin 2022 qui s'est déroulée au Grand Palais de Lille. Le Forum a été l'occasion de réunir autour du thème « *Shaping Europe's digital Future* » plusieurs personnalités dont Margrethe VESTAGE, Vice-présidente exécutive de la Commission européenne, Commissaire à la concurrence, Guillaume POUPARD, Directeur général de l'ANSSI, le Général Christian RODRIGUEZ, Directeur de la Direction Générale de la Gendarmerie Nationale (DGGN), ou encore Marie-Laure DENIS, Présidente de la CNIL.

Durant la séance inaugurale, Guillaume TISSIER, le président du FIC, a rappelé qu'il y avait urgence à ce que l'Europe se structure et se fédère autour des risques de cybersécurité. En effet, en tant que principal événement européen sur les questions de la sécurité et de confiance numérique, le Forum International de la Cybersécurité favorise la réflexion et l'échange au sein de l'écosystème européen de la cybersécurité.

Ce salon dédié a pour objet de faire face aux défis opérationnels de la cybersécurité et contribue à la construction d'un futur numérique conforme aux valeurs et aux intérêts européens.

Les agents de la CCIN qui étaient présents ont pu participer sous divers formats proposés pendant ces 3 jours à des séances plénières ou des tables-rondes portant sur « ***Comment sécuriser les identités numériques pour exploiter les données en toute confiance*** ». Il était également possible d'assister à des démonstrations de techniques de cyber-attaque, FIC Talk et masterclass. Ainsi, la CCIN a pu échanger sur de nombreux sujets tout au long du FIC, avec différents professionnels de la cybersécurité autour de la sécurité des données et de la transformation numérique.

Enfin, le Forum a été animé par 28 conférences réunissant des intervenants tels que l'Ambassade du Canada, Orange Cyberdefense, Cybervadis, WALLIX, Microsoft, Tehtris, Crowdstrike, NANO Corp, CONIX, Stormshield, OneTrust, Crowdsec, Digitemis, Fortinet, Trend Micro, Ping Identity, Blancco, MasterCard, AntemetA, Tenable, Tanium, Airbus, SANS Institute, Snyl, Capgemini Sogeti, Delinea et Thales.

La CCIN a également rencontré des experts cyber et des étudiants, et les a observés s'affronter lors de « *L'European Cyber Cup* » , 1ère compétition d'eSport dédiée au hacking éthique, véritable temps fort de ce forum.

**Réunion annuelle de l'Association francophone des Autorités de protection des données personnelles**

Le 3 octobre 2022 s'est déroulée à Tunis la 14ème conférence de l'Association francophone des Autorités de protection des données personnelles (AFAPDP), auxquelles 2 agents du Secrétariat ont participé.

Organisée par l'Instance nationale de protection des données à caractère personnel (INPDP), l'Autorité de protection des données tunisienne, cet évènement a permis aux représentants des Autorités membres de l'Association, de la société civile et des Organisations internationales de se retrouver après deux années marquées par la pandémie de Covid.

Trois thèmes étaient au programme : l'identité, entre autres numérique, qui soulève des problématiques en matière de protection des données personnelles et de souveraineté numérique des Etats, la coopération dans le domaine de la

protection des données personnelles, composante incontournable du travail des Autorités de protection des données personnelles, du fait même du caractère transfrontalier des flux d'informations traitées, et enfin, le traitement de la protection des données personnelles dans le cadre de l'aide internationale au développement.

Le lendemain de cette conférence, l'Association a tenu sa 13ème Assemblée générale, réservée aux membres et observateurs, au cours de laquelle ces derniers ont décidé, à l'unanimité, de renouveler leur confiance aux membres du Bureau en place, à l'exception du représentant de l'IDP albanaise, qui s'est retiré.

La composition du Bureau a été adoptée comme suit :

**Président :** Chawki GADDES, INPDP Tunisie
**Première Vice-Présidente :** Marguerite OUEDRAOGO, CIL Burkina Faso
**Deuxième Vice-Président :** Faustino Monteiro VARELA, CNPD Cap-Vert
**Troisième Vice-Présidente :** Catherine LENNMAN, PFPDT Suisse
**Secrétaire Générale :** Marie-Laure DENIS, CNIL France

Enfin, parallèlement à cette réunion, une session de formation animée par deux juristes de la Commission Nationale de l'Informatique et des Libertés (CNIL) sur les contrôles des systèmes d'identification était proposée aux agents investigateurs des Autorités membres.

**« *Les assises de la sécurité* » 2022 : 20ème édition**

Actuellement, parmi les risques numériques, particulièrement difficiles à appréhender et à détecter pour les entreprises mondiales, les cybermenaces permanentes demeurent en tête de liste.

Plus qu'un événement, « *Les Assises de la Sécurité* » organisées par Comexposium sous la direction de Maria IACONO, se sont déroulées **du 12 au 15 octobre 2022** au Grimaldi Forum de Monaco. Cet événement accompagne tous les acteurs du marché depuis 20 ans. Un lieu de rencontre unique pour s'interroger sur les problématiques actuelles et futures du cyber. Les Assises de la Sécurité sont le rendez-vous incontournable des experts de la cybersécurité à l'échelle mondiale. Ainsi, pour la 20ème édition, des Assises, près de 3 000 participants (RSSI, fournisseurs...) et 164 sociétés (PME, start-ups, grands groupes...) étaient présents et la CCIN aussi !

La session 2022 des Assises de la Sécurité, s'est ouverte avec le discours de Guillaume POUPARD, Directeur Général de l'ANSSI qui a souligné que « *Notre cybersécurité ne passe pas par un domaine d'excellence mais la capacité à traiter une mosaïque complexe de sujets* », dans un contexte marqué par des challenges persistants liés à une géopolitique plus que jamais propice

aux cyberattaques. Il s'est également exprimé sur plusieurs grands sujets d'actualité cyber : rançongiciels, attaques par déni de service, sabotage informatique, cyber espionnage qui font désormais régulièrement partie du quotidien des entreprises et des administrations.

Durant cet évènement la CCIN a pu échanger avec des dirigeants cybersécurité d'entreprises françaises et des fournisseurs de solutions et services technologiques au travers d'un programme de contenus experts, apportant vision stratégique et opérationnelle, et des retours d'expérience.

A cette occasion, les agents de la CCIN ont pu participer à des conférences sur « *L'intelligence artificielle au service de la cybersécurité* », des tables rondes sur les indicateurs de performance au service de la cybersécurité ou encore un atelier portant sur la sensibilisation des utilisateurs et un retour d'expérience sur les bonnes pratiques à avoir.

Enfin la conférence s'est clôturée par une table ronde entre Christian-Marc LIFLÄNDER, Head Cyber and Hybrid Policy Section, Emerging Security Challenges Division, NATO Headquarters, Brussels, Guillaume POUPARD, Directeur Général, ANSSI et Thierry AUGER, Président des Assises 2022 et Corporate CIO & Group CISO, Lagardère.

**Participation virtuelle à la 44ème conférence de l'Assemblée mondiale pour la protection de la vie privée**

Du 25 au 28 octobre, un agent du Secrétariat a participé de manière virtuelle à la 44ème conférence de l'Assemblée mondiale pour la protection de la vie privée (AMVP) qui s'est tenue cette année à Istanbul dans un format hybride.

Cet évènement international qui a eu lieu pour la première fois en 1979, est constitué d'une séance ouverte à tous les experts dans le domaine de la protection des données puis d'une session fermée réservée aux Autorités de protection des données, ainsi que de plusieurs évènements parallèles.


Intitulée cette année « ***A Matter of Balance: Privacy in the Era of Rapid Technological Advancements*** », la conférence s'est focalisée sur la nécessité de trouver un équilibre entre le respect de la vie privée et les avancées toujours plus rapides des technologies.

De très nombreux sujets d'actualité ont ainsi été abordés, allant de l'intelligence artificielle au métaverse en passant par la reconnaissance faciale, la blockchain et la surveillance de masse.

**Symposium sur la cybersécurité et la protection des données dans l'action humanitaire**

Un agent du Secrétariat a été invité à participer le 8 novembre à un symposium d'une journée sur la cybersécurité et la protection des données dans l'action humanitaire, organisé par le Ministère des Affaires étrangères et européennes du Luxembourg, la Commission Nationale de la Protection des Données (CNPD), Securitymadein.lu, l'Université du Luxembourg, la Croix-Rouge luxembourgeoise et le Comité International de la Croix-Rouge (CICR).

Au cours de la journée, les participants, répartis dans différents groupes de travail, ont examiné un certain nombre de défis juridiques, politiques et techniques soulevés par la numérisation et la transformation numérique dans l'action humanitaire, avec un accent particulier sur la cybersécurité et la protection des données afin de proposer des perspectives et des solutions possibles.

Les personnes présentes (principales parties prenantes des organisations humanitaires, des gouvernements, des autorités de protection des données, des agences de cybersécurité, du secteur privé, de la société civile et du monde universitaire) ont ainsi discuté autour de trois thèmes principaux :

- normes et principes communs pour les données humanitaires ;
- vers la construction d'un espace humanitaire numérique sûr et de confiance ;
- opérationnalisation de la protection des données et de la cybersécurité dans l'action humanitaire.


# FICHES PRATIQUES


## Fiche métier du Délégué à la Protection des Données

Qualifié par le Groupe de travail « *Article 29* » (GT art. 29)[1] comme étant « *l'une des pierres angulaires du régime de responsabilité* », le Délégué à la Protection des Données (DPD) devrait devenir en Principauté, en vertu de la future[2] législation sur la protection des données personnelles monégasque, un **acteur clé** dans le système de gouvernance desdites données.

Obligatoire dans certains organismes et souvent recommandé dans d'autres, le projet de Loi prévoit en effet que le DPD doit **faciliter le respect de la législation en matière de protection des données** et agir à la fois comme **l'interlocuteur privilégié** pour toutes les questions relatives aux

données personnelles, qu'elles soient internes ou bien qu'elles émanent d'une personne concernée, et comme le **correspondant de l'Autorité de protection.**

La présente fiche pratique a ainsi vocation à présenter ce nouveau métier.

**Dans quel cas un Délégué à la Protection des Données doit-il impérativement être nommé ?**

Le projet de Loi prévoit qu'à l'exception des juridictions dans l'exercice de leurs fonctions juridictionnelles (pour lesquelles un Délégué spécifique doit être nommé), la désignation d'un Délégué à la Protection des Données est obligatoire dans les cas suivants :

- le traitement de données est effectué par une personne morale de droit public ou une personne morale de droit privé investie d'une mission d'intérêt général ou concessionnaire de service public ;

- les activités de base du responsable de l'organisme consistent en des opérations de traitement qui, du fait de leur nature, de leur portée ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées.

**Quid de la notion de suivi régulier et systèmatique**

Selon les « *Lignes directrices concernant les délégués à la protection des données* » adoptées par le Groupe de travail « *Article 29* » le 13 décembre 2016, le terme « ***régulier*** » doit s'entendre comme :

- continu ou se produisant à intervalles réguliers au cours d'une période donnée ; ou
- récurrent ou se répétant à des moments fixes ; ou
- ayant lieu de manière constante ou périodique.

Le terme **« *systématique* »** s'entend quant à lui comme :
- se produisant conformément à un système ; ou
- préétabli, organisé ou méthodique ; ou
- ayant lieu dans le cadre d'un programme général de collecte de données ; ou
- effectué dans le cadre d'une stratégie.

**Exemples :** activité de marketing dont la personnalisation est fondée sur les données personnelles, profilage et notation à des fins d'évaluation des risques ou encore géolocalisation par des applications mobiles.

[1] Groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 (avant l'entrée en vigueur du Règlement Général sur la Protection des Données - RGPD).
[2] Cette Fiche pratique a été rédigée à l'aune du projet de Loi relative à la protection des données personnelles, et sera modifiée selon les dispositions du texte définitif lorsqu'il sera adopté.

- les activités de base de l'organisme consistent en un traitement **à grande échelle de données sensibles ou de données à caractère personnel relatives à des condamnations pénales ou à des infractions.**

***Quid de la notion de traitement à grande échelle***

*Si elles ne fournissent aucune définition de cette notion, les « Lignes directrices concernant les délégués à la protection des données » recommandent néanmoins de prendre en compte les facteurs suivants afin de déterminer si un traitement est mis en œuvre à grande échelle :*

- *le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée ;*
- *le volume de données et/ou le spectre des données traitées ;*
- *la durée, ou la permanence des activités de traitement des données ;*
- *l'étendue géographique de l'activité de traitement.*

***Exemples :** traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités, traitement des données de voyage des passagers utilisant un moyen de transport public urbain ou encore traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités.*


Dans tous les autres cas, même si cela n'est pas obligatoire, il est recommandé de **désigner un Délégué à la protection des données** dès lors qu'un organisme est **confronté à des problématiques liées à la protection des données personnelles.**

**Qui peut être nommé Délégué à la protection des données ?**

*Les qualifications*

**Aucune qualification** spécifique n'est requise pour être Délégué à la protection des données.

En pratique, toutefois, le Délégué à la protection des données doit impérativement disposer des **compétences** et **connaissances adéquates,** notamment en droit et sécurité informatique des données personnelles, pour exercer ses missions. Ce niveau d'expertise doit être **proportionné** à la sensibilité, à la complexité et au volume des données traitées par l'organisme.

Il est important par ailleurs que le Délégué à la protection des données ait une **bonne compréhension** des opérations de traitement effectuées par l'organisme, des systèmes d'informations utilisés par ledit organisme et des besoins de celui-ci en matière de protection des données.

L'organisme doit également permettre au Délégué à la protection des données **d'entretenir et compléter ses compétences et connaissances** (formation continue, participation à des ateliers, ...) pendant toute la durée de sa mission.

*Les risques de conflits d'intérêts*

La fonction de Délégué à la protection des données n'est pas forcément un emploi à temps plein. Il arrive en effet que celui-ci soit nommé à temps partiel et exerce d'autres fonctions au sein de l'organisme. Aussi, afin d'éviter que le Délégué à la protection des données ne soit « *juge et partie* », l'organisme doit s'assurer **qu'il ne dispose d'aucun pouvoir décisionnel** sur la détermination des finalités et moyens de traitements.

Ce risque de conflits d'intérêts s'apprécie « *au cas par cas* » en fonction des activités, de la taille et de la structure de l'organisme.

Il est donc recommandé de procéder à un recensement des fonctions incompatibles avant de procéder à la nomination d'un Délégué à la protection des données.

A titre d'exemples, les fonctions suivantes sont plus susceptibles que d'autres d'entraîner un conflit d'intérêts : directeur général, directeur financier, directeur des opérations, directeur des ressources humaines ou encore responsable de la sécurité des systèmes d'information (RSSI).

*Les cas particuliers*

Un seul Délégué à la protection des données peut être désigné pour plusieurs personnes morales de droit public ou pour plusieurs personnes morales de droit privé investies d'une mission d'intérêt général ou concessionnaires d'un service public.

De même, un groupe d'entreprises peut désigner un seul Délégué à la protection des données à condition que celui-ci soit facilement joignable à partir de chaque lieu d'établissement.

Enfin, la fonction de Délégué à la protection des données peut être exercée par une personne physique ou morale externe (consultant, cabinet d'avocats, cabinet de conseil, ...).

**Quelles sont les missions du Délégué à la protection des données ?**

Les missions du Délégué à la protection des données consistent à accompagner, informer et conseiller l'organisme afin que celui-ci soit en conformité avec la législation monégasque en matière de protection des données.

Il a par ailleurs pour mission de coopérer avec l'Autorité de protection.

Enfin, le Délégué à la protection des données désigné par l'Etat doit également présenter à l'Autorité de protection des dossiers de demande d'avis pour tout traitement relatif à la souveraineté de l'Etat.

Les missions du Délégué à la protection des données sont ainsi au nombre de 5 :

- **informer et conseiller** l'organisme ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la législation ;
- **s'assurer** du respect de la législation en matière de protection des données personnelles ainsi que les règles internes de l'organisme en matière de protection des données personnelles ;


- **dispenser des conseils**, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données personnelles ;
- **coopérer** avec l'Autorité de protection et être son correspondant sur les questions relatives au traitement ;
- **présenter à l'Autorité de protection les demandes d'avis** lorsqu'elles portent sur les traitements suivants :

• les traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;

• les traitements mis en œuvre par les autorités administratives et judiciaires, agissant dans le cadre de leurs prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

Pour l'accomplissement de ces missions, le Délégué à la protection des données doit impérativement **tenir compte du risque associé aux opérations de traitement** compte tenu de la nature, de la portée, du contexte et des finalités.

**Comment le Délégué à la protection des données exerce-t-il ses missions ?**

*Les garanties*

Afin de permettre aux Délégués à la protection des données de mener à bien les missions pour lesquelles ils ont été nommés, plusieurs garanties sont mises en place.

C'est ainsi que le Délégué à la protection des données doit tout d'abord pouvoir **agir en toute indépendance.** Pour cela, il ne doit recevoir d'instructions


d'aucune autorité en ce qui concerne l'exercice de ses missions. Un dirigeant ne peut donc pas, par exemple, indiquer au Délégué à la protection des données quel résultat doit être obtenu ou quelle interprétation d'une disposition législative en matière de protection des données doit être retenue.

Cette indépendance ne signifie toutefois pas que le Délégué à la protection des données dispose de pouvoirs de décision allant au-delà des missions qui lui sont confiées.

Le Délégué à la protection des données doit par ailleurs **disposer de ressources suffisantes.** Outre l'octroi de moyens financiers nécessaires et d'infrastructures (locaux, équipements, ...) adéquates, cette garantie comprend également le soutien actif du Délégué à la protection des données par l'encadrement supérieur, un temps nécessaire, notamment lorsque le Délégué à la protection des données est à temps partiel, pour accomplir ses missions, ou encore un accès facilité aux autres services (service des ressources humaines, service juridique, DSI, ...) pour l'obtention des informations dont il a besoin.

Le Délégué à la protection des données doit aussi **être associé**, d'une manière appropriée et en temps utile, **à toutes questions relatives à la protection des données.** L'organisme devra donc veiller à inviter le Délégué à la protection des données à toutes réunions utiles et à prendre son avis avant toute décision ayant un impact sur la protection des données personnelles. Il devra également le consulter immédiatement en cas de violation de données ou de tout autre incident.

L'organisme doit en outre donner au Délégué à la protection des données l'accès aux données et aux opérations de traitement, à l'exception :

- des traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
- des traitements qui intéressent la sécurité nationale.

Le Délégué à la protection des données **ne peut être relevé de ses fonctions ou pénalisé** par l'organisme pour l'exercice de ses missions. Concrètement, cela signifie qu'il ne pourra pas par exemple être relevé de ses fonctions pour avoir conseillé à l'organisme de faire une analyse d'impact pour un traitement de données qu'il considère susceptible d'engendrer un risque élevé pour la protection des données personnelles.

Enfin, le Délégué à la protection des données **ne peut être tenu responsable du non-respect par l'organisme de la législation sur la protection des données.** C'est en effet l'organisme qui reste tenu de s'assurer et d'être en mesure de démontrer

que le traitement est conforme à la législation sur la protection des données. En conséquence, si l'organisme prend des décisions contraires à l'avis du Délégué à la protection des données, celui-doit pouvoir faire part clairement de son opinion divergente auprès de l'encadrement supérieur.

*Les obligations*

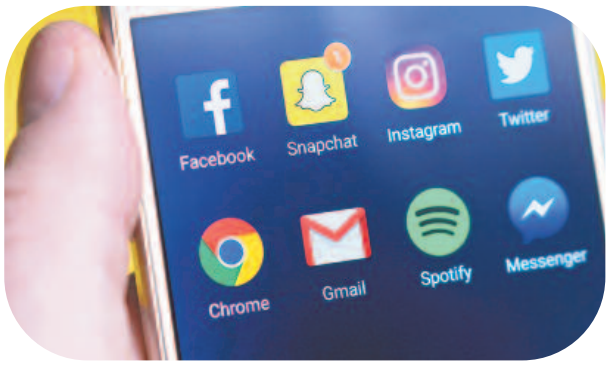
En contrepartie de toutes ces garanties, le Délégué à la protection des données est également tenu à certaines obligations.

La toute première d'entre elles est une **obligation de confidentialité** en ce qui concerne l'exercice de ses missions.

Le Délégué à la protection des données doit également **faire preuve d'intégrité et d'un haut niveau de déontologie** afin de promouvoir et de faire respecter la protection des données personnelles au sein de l'organisme dans lequel il exerce ses fonctions.

Enfin, le Délégué à la protection des données **doit être joignable**, soit en étant physiquement dans le même lieu que les employés, soit au travers d'un service d'assistance téléphonique ou de tout autre moyen de communication sécurisé, afin que les personnes concernées puissent prendre contact avec lui. A cet égard, il appartient à l'organisme de publier les coordonnées professionnelles du Délégué à la protection des données et de les communiquer à l'Autorité de protection.

## Comment récupérer un compte Facebook, Instagram ou TikTok piraté ?




Depuis quelques années, la CCIN reçoit de plus en plus d'appels de particuliers, de professionnels ou d'Associations qui se sont fait pirater leur(s) compte(s) Facebook, Instagram et/ou TikTok.

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

Aussi afin d'aider les personnes victimes de piratage sur ces trois réseaux sociaux, la CCIN a souhaité publier un petit guide des procédures de réinitialisation du mot de passe ou de récupération de compte.

### COMPTE FACEBOOK PIRATÉ

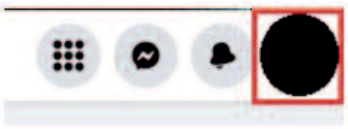
Deux cas de figure sont à envisager selon que votre compte est toujours accessible ou ne l'est plus.

## Cas de figure n° 1 : Vous pouvez toujours vous connecter à votre compte Facebook

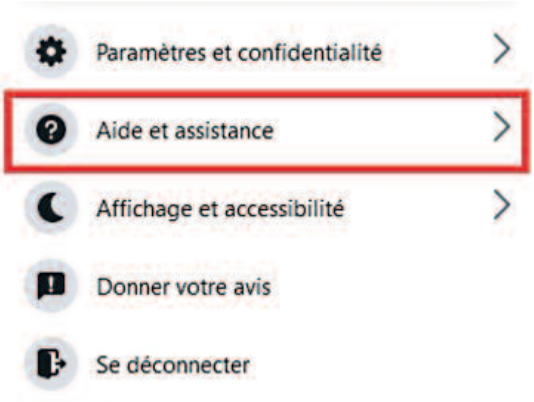
Si votre compte est toujours accessible, il convient de lancer une procédure de réinitialisation du mot de passe.

Cette procédure est la suivante :

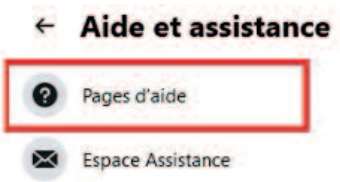
- Sur votre PC, connectez-vous à votre compte Facebook.
- Postez un message sur votre mur afin d'informer vos connaissances que votre compte a été piraté. Vous pouvez également, à la place, les contacter par message privé.
- En haut de votre page, dans la barre de menu à droite, cliquez sur la flèche pointant vers le bas.



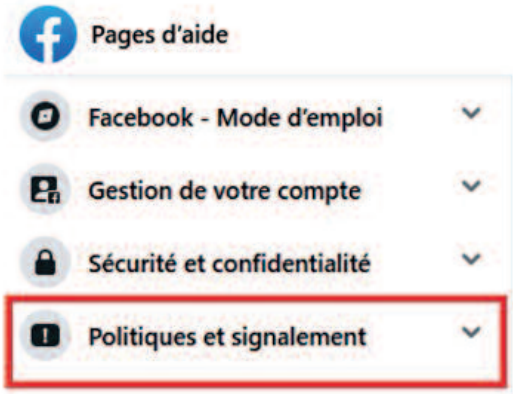
- Un menu déroulant apparaît. Cliquez alors sur **Aide et assistance.**




- Cliquez ensuite sur **Pages d'aide.**

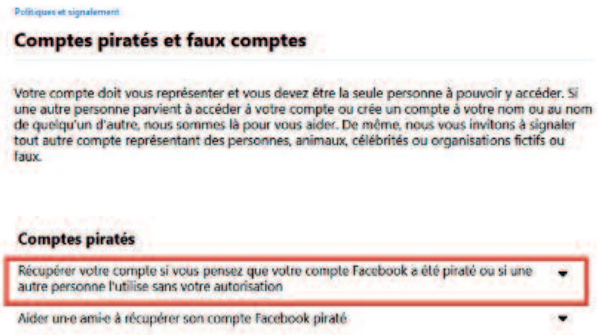



Dans le menu déroulant, sélectionnez Politiques et signalement.

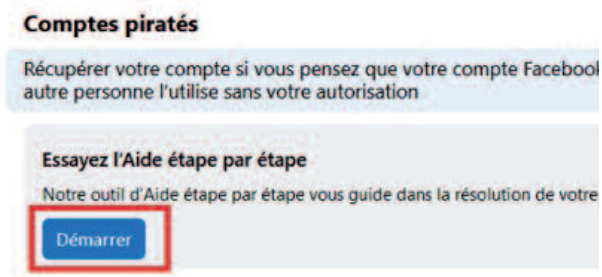



- Un nouveau menu déroulant apparaît. Cliquez sur Comptes piratés et faux comptes.

• Une nouvelle page apparaît. Sélectionnez **Récupérer votre compte si vous pensez que votre compte Facebook a été piraté ou si une autre personne que vous l'utilise sans votre autorisation.**




• Cliquez sur **Démarrer.**




A partir de là, Facebook va vous accompagner étape par étape pour vous permettre de réinitialiser votre mot de passe.

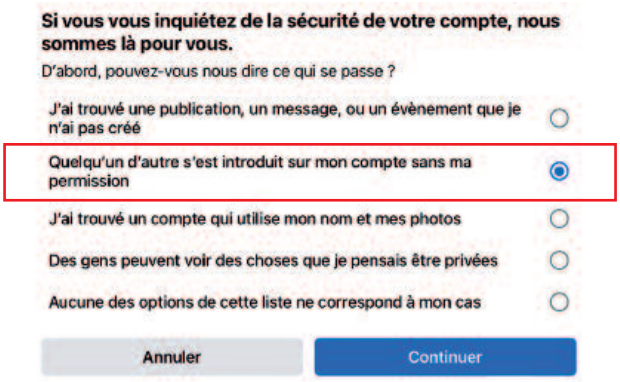
## Cas de figure n° 2 : Vous ne pouvez plus vous connecter à votre compte Facebook

Si votre adresse e-mail ou votre mot de passe a été modifié, il convient de lancer une procédure de récupération de compte.

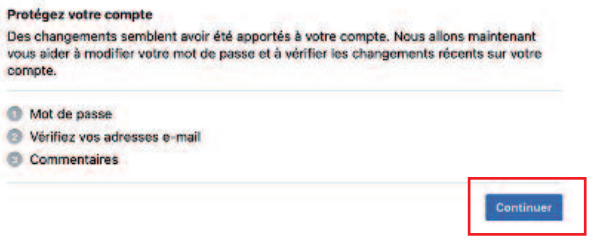
Cette procédure est la suivante :

• Avec votre navigateur Web, allez sur la page spéciale Facebook Hacked (**https://www.facebook.com/hacked**).

• Une page apparaît. Cochez **Quelqu'un d'autre s'est introduit sur mon compte sans ma permission** puis cliquez sur Continuer.




• Une page s'ouvre. Cliquez sur **Continuer.**




A partir de là, Facebook va vous accompagner étape par étape pour vous permettre de réinitialiser votre mot de passe et récupérer votre compte.

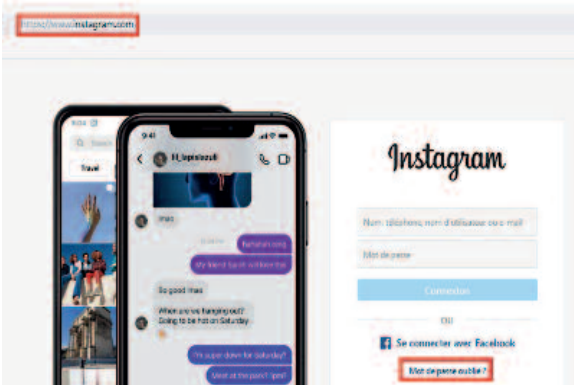
## COMPTE INSTAGRAM PIRATÉ

Deux cas de figure sont à envisager. Dans le cas le moins grave vous avez toujours accès à votre compte ou si vous ne pouvez plus y accéder, seul votre mot de passe a été modifié. Dans le cas le plus grave, votre compte est devenu inaccessible car le pirate a modifié certaines de vos informations dont votre adresse e-mail.

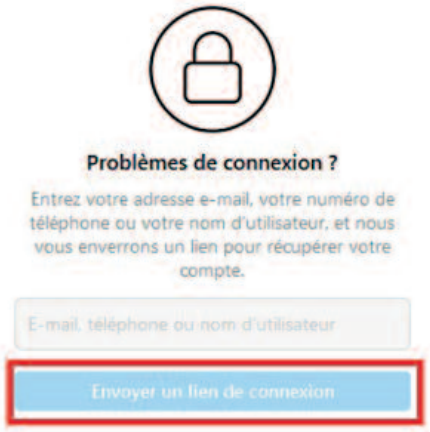
### Cas de figure n° 1 : Vous pouvez toujours vous connecter à votre compte Instagram ou vous ne pouvez plus y accéder car votre mot de passe a été modifié

Il convient de suivre la **procédure de réinitialisation du mot de passe.**

- Sur votre téléphone portable, rendez-vous sur la page d'accueil d'Instagram (https://www.instagram.com) et cliquez sur Mot de passe oublié ? (iPhone) ou Obtenir de l'aide pour se connecter (Android)




- Saisissez l'adresse e-mail, le numéro de téléphone ou le nom d'utilisateur associé à votre compte, puis appuyez sur **Envoyer un lien de connexion.**

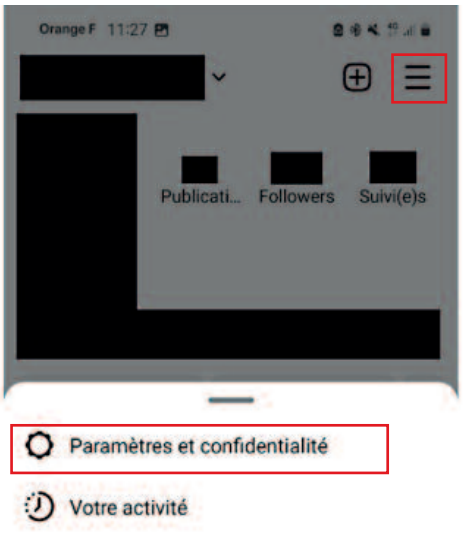



- Instagram vous enverra alors un lien pour que vous puissiez récupérer votre compte. Vérifiez votre boîte e-mail ou votre téléphone portable et cliquez sur le lien de connexion envoyé.

A partir de là, il suffira de suivre les instructions à l'écran.

Une fois votre compte récupéré, il est important de vérifier vos informations personnelles en suivant la procédure suivante :

- Allez dans Paramètres et confidentialité en haut à droite de votre page de profil.



• Une page apparaît. Cliquez sur **Espace Comptes.**

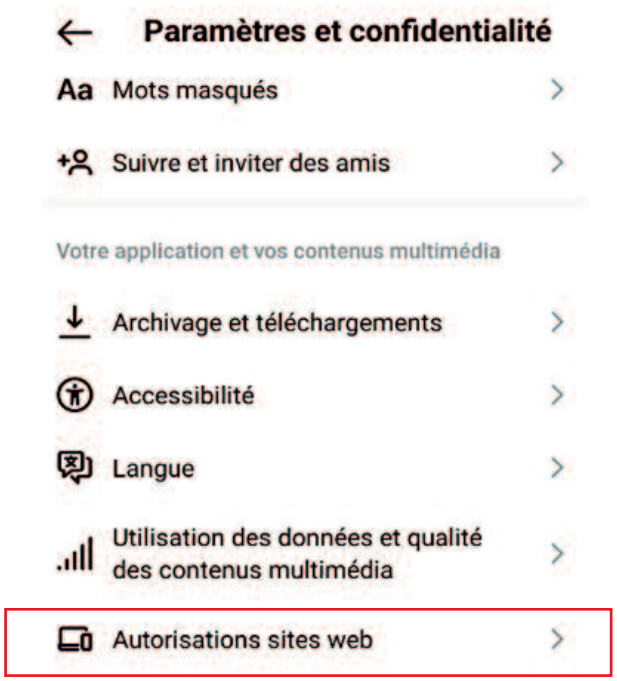

• Une page s'ouvre. Cliquez sur **Informations personnelles.**


Cette nouvelle page vous permet de vérifier que le numéro de téléphone ainsi que l'adresse e-mail indiqués dans les paramètres sont les bons.

Après la vérification de vos informations personnelles, il est important de sécuriser votre compte en annulant l'accès de certaines applications tierces audit compte.
Pour vérifier les accès accordés, il suffit de suivre la procédure suivante :

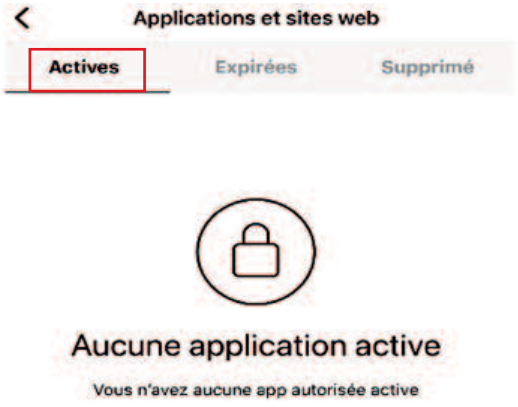
• Allez dans **Paramètres et confidentialité** en haut à droite de votre page de profil.

- Une page apparaît. Cliquez sur **Autorisations sites web.**




- Une page s'ouvre. Cliquez sur **Applications et sites web.**


- Les applications autorisées à accéder à votre compte sont listées dans la section **Actives**. Un simple clic de souris suffit pour révoquer l'accès à une application.





## Cas de figure n° 2 : Vous ne pouvez plus vous connecter à votre compte Instagram car votre adresse e-mail a été modifiée

- La première étape est de consulter votre boite e-mail (celle que vous avez utilisée pour créer votre compte Instagram) pour voir si vous avez reçu un message d'Instagram.
- Si vous avez reçu un e-mail d'Instagram (security@mail.instagram.com) vous informant que votre adresse e-mail a été modifiée, vous pouvez annuler cette action à l'aide de l'option **Sécuriser mon compte** disponible dans ce message.
- Plusieurs options de récupération pourront vous être proposées en fonction de votre compte et de votre sécurité :

➢ envoyer une photo de vous tenant une copie manuscrite du code que Instagram vous a fourni.

➢ envoyer l'adresse e-mail ou le numéro de mobile utilisé pour vous inscrire et le type d'appareil utilisé au moment de l'inscription (par exemple : iPhone 12, Samsung S20, iPad 9 ou autre).

Lorsque Instagram sera convaincu que vous êtes bien le propriétaire du compte, vous en serez informé par e-mail.

- Si d'autres informations ont également été modifiées (par exemple, votre mot de passe) et que vous ne pouvez pas annuler le changement de votre adresse e-mail, demandez un lien de connexion ou un code de sécurité à Instagram
- Pour confirmer que le compte vous appartient, vous pouvez demander à recevoir un lien de connexion sur votre boîte e-mail ou votre téléphone.

➢ Sur l'écran de connexion, appuyez sur Obtenez de l'aide pour vous connecter (Android) ou **Mot de passe oublié ?** (iPhone ou navigateur web).

➢ Saisissez le nom d'utilisateur, l'adresse e-mail ou le numéro de téléphone associé à votre compte, puis appuyez sur Suivant.


Si vous n'avez pas accès au nom d'utilisateur, à l'adresse e-mail ou au numéro de téléphone associé à votre compte, saisissez les dernières informations de connexion que vous avez utilisées, puis appuyez sur **Vous ne parvenez pas à réinitialiser votre mot de passe ?** sous le bouton **Suivant** et suivez les instructions qui s'affichent à l'écran.

➢ Choisissez votre adresse e-mail ou votre numéro de téléphone, puis appuyez sur **Suivant**.

➢ Cliquez sur le lien de connexion de votre e-mail ou le texto (SMS) et suivez les instructions qui s'affichent à l'écran.

- Si vous ne parvenez pas à récupérer l'accès à votre compte avec le lien de connexion envoyé, vous pouvez demander un code de sécurité à Instagram ou une assistance supplémentaire.

### POUR IPHONE

- Sur l'écran du lien de connexion, appuyez sur **Vous ne parvenez pas à réinitialiser votre mot de passe ?** sous Envoyer un lien de connexion. Saisissez votre adresse e-mail ou votre numéro de téléphone, puis appuyez sur Envoyer le code de sécurité.

- Si vous ne recevez pas de code de sécurité, appuyez sur **Je n'ai pas accès à cette adresse e-mail ni à ce numéro de téléphone** sous **Envoyer le code de sécurité**, puis suivez les instructions à l'écran.

### POUR ANDROID

- Sur l'écran de connexion, appuyez sur **Obtenez de l'aide pour vous connecter** sous **Connexion.**
- Saisissez le nom d'utilisateur, l'adresse e-mail ou le numéro de téléphone associé à votre compte, puis appuyez sur **Vous ne parvenez pas à réinitialiser votre mot de passe ?** Si vous avez plusieurs comptes Instagram, il conviendra de sélectionner le compte concerné par le piratage, puis de suivre les instructions à l'écran.

- Appuyez sur **Besoin d'une aide supplémentaire ?** et suivez les instructions à l'écran.
- Saisissez votre adresse e-mail ou votre numéro de téléphone, puis appuyez sur **Envoyer le code de sécurité.**
- Si vous ne recevez pas de code de sécurité, appuyez sur **Je n'ai pas accès à cette adresse e-mail ni à ce numéro de téléphone** sous **Envoyez le code de sécurité**, puis suivez les instructions à l'écran.

Assurez-vous de fournir une nouvelle adresse e-mail qui n'est associée à aucun compte Instagram/Facebook.

En cas de demande d'assistance supplémentaire, Instagram peut vous demander de confirmer votre identité :

- **Si le compte Instagram ne comporte pas de photos de vous :** Vous allez recevoir un e-mail de réponse automatique de la part de l'équipe assistance de Meta. Il vous sera alors demandé de confirmer votre identité en fournissant :
  - l'adresse e-mail ou le numéro de téléphone utilisé lors de la création du compte ;
  - le type d'appareil utilisé au moment de l'inscription (par exemple, iPhone, Android, iPad).
- **Si le compte Instagram comporte des photos de vous**, il conviendra de prendre un selfie vidéo de vous en tournant la tête dans différentes directions afin de vérifier que vous êtes une personne réelle et de confirmer votre identité.
  - Après vérification de votre identité vous recevrez un e-mail de la part d'Instagram à l'adresse e-mail sécurisée que vous avez renseignée.
  - Ce selfie vidéo ne sera jamais publié et sera supprimé dans un délai de 30 jours.
  - Si votre identité n'a pu être confirmée, vous pouvez recommencer en envoyant une nouvelle vidéo.

**Quelques conseils pour bien sécuriser votre compte, une fois celui-ci récupéré**

- **Choisissez un mot de passe fort.** Utilisez une combinaison d'au moins six chiffres, lettres et signes de ponctuation (tels que ! et &). Ce mot de passe doit être différent des autres mots de passe que vous utilisez ailleurs sur Internet.
- **Changez de mot de passe régulièrement**, en particulier si vous recevez un message d'Instagram vous invitant à le faire.
- **Ne communiquez jamais votre mot de passe** à une personne que vous ne connaissez pas ou en laquelle vous n'avez pas confiance.
- **Activez l'authentification à deux facteurs.**
- **Assurez-vous que votre boîte e-mail est sécurisée.** Toute personne qui peut lire votre e-mail peut probablement également accéder à votre compte Instagram. Changez le mot de passe de vos comptes de messagerie électronique et assurez-vous d'utiliser un mot de passe différent pour chacun d'eux.
- **Déconnectez-vous d'Instagram lorsque vous partagez un ordinateur ou un téléphone avec d'autres personnes.** Sur un ordinateur public, ne cochez jamais la case « *Mémoriser* ». Cette option vous permet en effet de rester connecté(e) même lorsque vous avez fermé la fenêtre du navigateur.

## COMPTE TIKTOK PIRATÉ

Si votre compte TikTok a été piraté, notamment si vous constatez des comportements suspects, il convient de le protéger !

Exemples de comportements suspects :

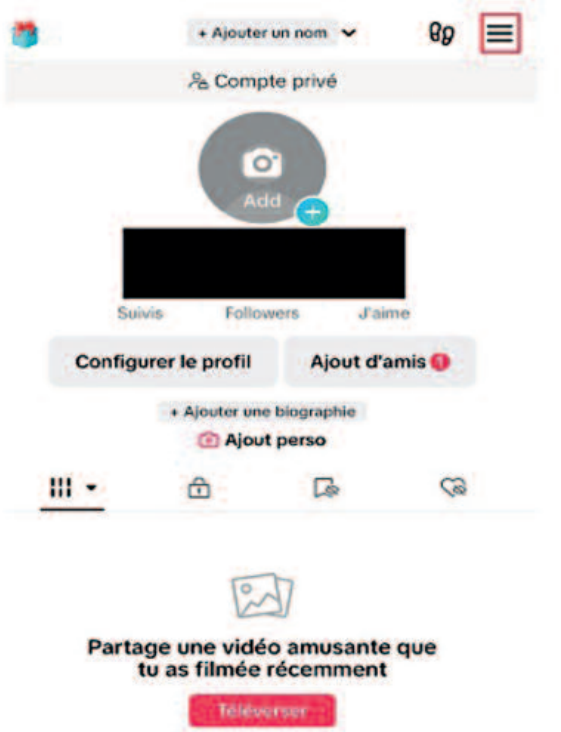
- le mot de passe ou le numéro de téléphone de votre compte a été modifié ;
- le nom d'utilisateur ou le surnom de votre compte a été modifié ;
- des vidéos ont été supprimées ou publiées sans votre accord ;
- des messages que vous n'avez pas écrits ont été envoyés sur votre compte.

Les 3 recommandations pour protéger votre compte sont les suivantes :

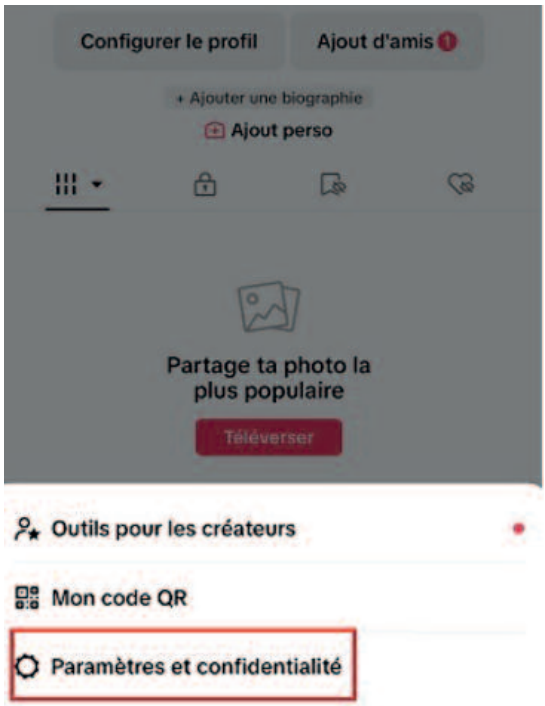
### 1. Réinitialisez votre mot de passe

Pour réinitialiser votre mot de passe il convient de cliquer sur Profil en bas à droite de votre écran.


Une page s'ouvre avec votre compte. Cliquez sur le « ***bouton hamburger*** » (trois lignes horizontales parallèles) en haut à droite de votre écran.



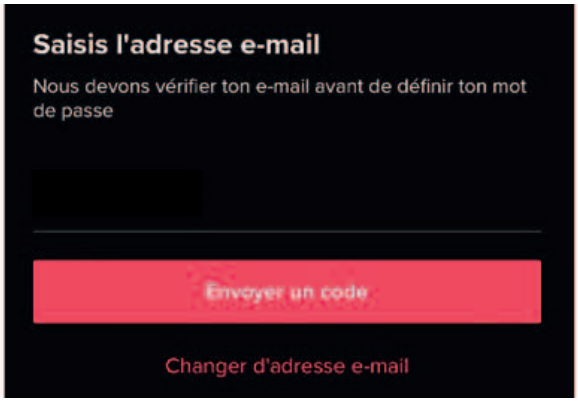

Une liste s'ouvre en bas de l'écran. Appuyez sur **Paramètres et confidentialité.**



Une liste déroulante s'ouvre. Cliquez sur **Compte.**

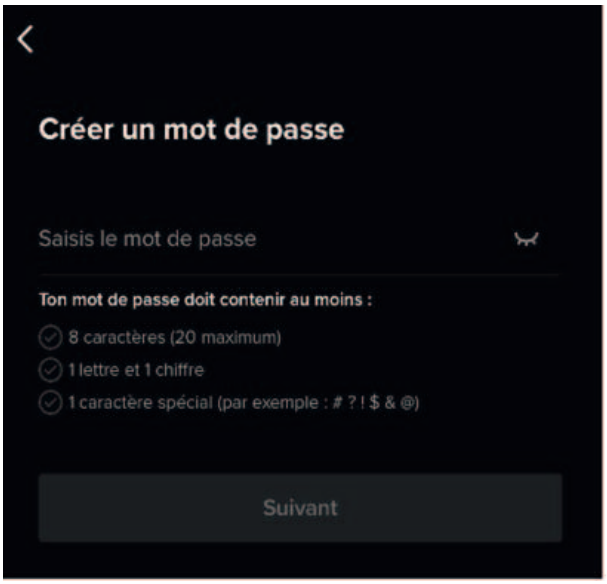

Sélectionnez **Mot de passe**.


Une nouvelle page apparaît vous demandant de saisir votre adresse e-mail.
Saisissez votre adresse puis cliquez sur Envoyer un code, afin de vérifier votre adresse.




Vous avez alors 1 minute pour taper le code à 6 chiffres qui vous a été envoyé sur votre adresse e-mail. Passé ce délai, le code ne sera plus valable.


Après insertion du code, une nouvelle page s'ouvre, vous demandant de créer un nouveau mot de passe.

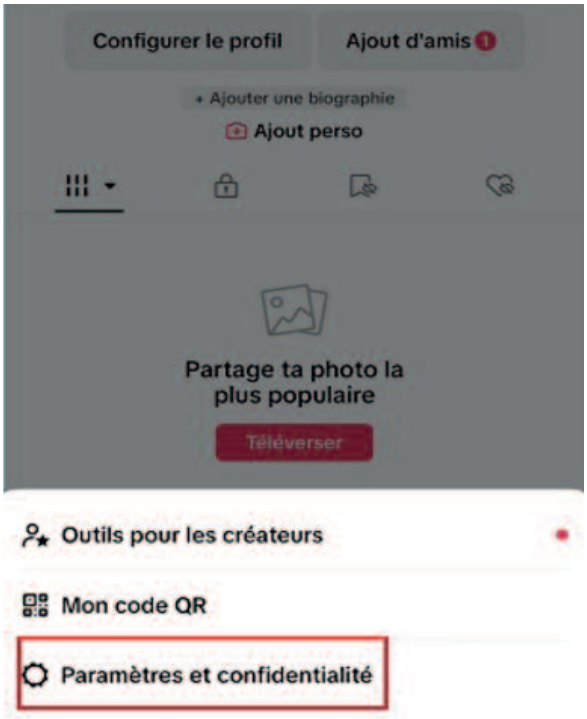


## 2. Associez un numéro de téléphone

Pour associer un numéro de téléphone à votre compte, il convient de cliquer sur Profil en bas à droite de votre écran.

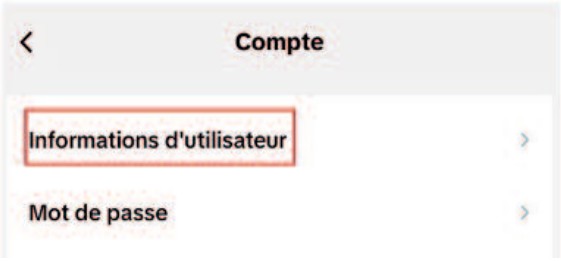

Une page s'ouvre avec votre compte. Cliquez sur le **« bouton hamburger »** (trois lignes horizontales parallèles) en haut à droite de votre écran.


Une liste s'ouvre en bas de l'écran. Appuyez sur **Paramètres et confidentialité.**

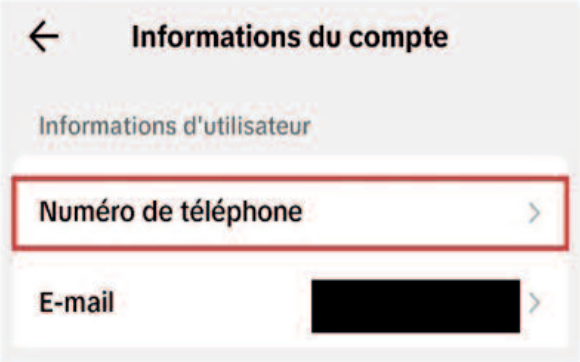



Une liste déroulante s'ouvre. Cliquez sur **Compte.**

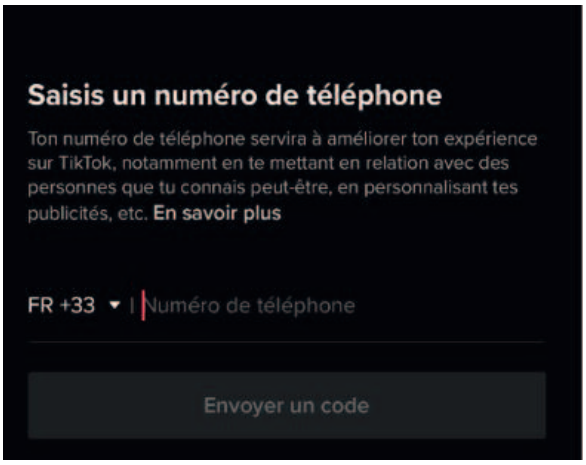

Une nouvelle page s'ouvre. Cliquez sur **Informations d'utilisateur**



Sélectionnez **Numéro de téléphone.**




Ajoutez votre numéro de téléphone sur la nouvelle page qui s'ouvre.

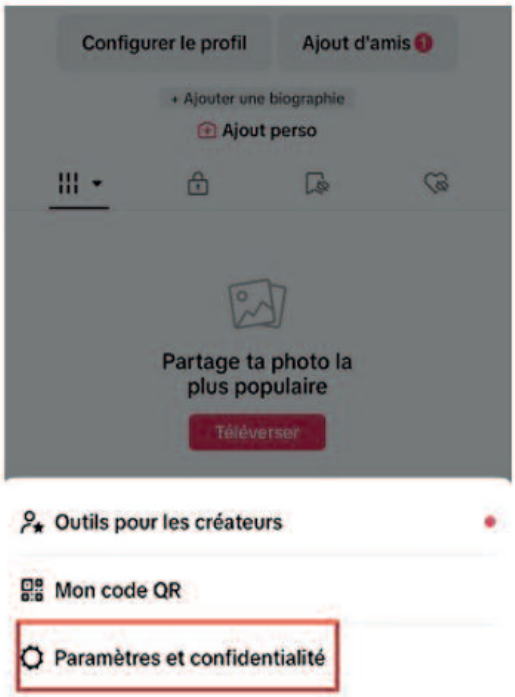



### 3. Supprimez les appareils suspects

Pour supprimer les appareils suspects qui sont connectés à votre compte TikTok, il convient de cliquer sur **Profil** en bas à droite de votre écran.


Une page s'ouvre avec votre compte. Cliquez sur le « ***bouton hamburger*** » (trois lignes horizontales parallèles) en haut à droite de votre écran.


Une liste s'ouvre en bas de l'écran. Appuyez sur **Paramètres et confidentialité**.



Une liste déroulante apparaît.
Cliquez sur **Sécurité.**


Une nouvelle page apparaît. Cliquez sur **Tes appareils.**


Supprimez dans la liste tous les appareils qui vous apparaissent suspects

Si, après avoir suivi ces étapes, votre problème n'a toujours pas été résolu, vous pouvez envoyer un e-mail à feedback@tiktok.com en indiquant les informations suivantes :

- **le nom d'utilisateur : @compte ;**
- **la date d'inscription : mois / année ;**
- **le lieu d'enregistrement : ville / pays ;**
- **le modèle de téléphone associé au compte : iPhone, Samsung, etc. ;**
- **le numéro de téléphone associé au compte ;**
- **l'adresse e-mail associée au compte ;**
- **le nom d'utilisateur et la capture d'écran de la page de profil des comptes Facebook / Instagram / Twitter / Google reliés à votre compte TikTok.**

Ces informations permettront aux équipes spécialisées de TikTok de vous apporter une aide adaptée à votre situation.

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

RAPPORT D'ACTIVITÉ
PUBLIÉ EN APPLICATION DE L'ARTICLE 2-14 DE LA LOI N° 1.165
RELATIVE À LA PROTECTION DES INFORMATIONS NOMINATIVES

www.silebleu.mc - Photo : Istockphoto, Freepik, Shutterstock, Gioia, Pexel.

Commission de Contrôle des Informations Nominatives - 14ème Rapport d'Activité Annuel 2022

CCIN

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

Le Concorde - 11 rue du Gabian
98000 Monaco
Tél. : +377 97 70 22 44
ccin@ccin.mc - www.ccin.mc