RAPPORT D'ACTIVITÉ

CCIN

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

2023

15ème rapport public

RAPPORT D'ACTIVITE PUBLIE EN APPLICATION DE L'ARTICLE 2-14 DE LA LOI N° 1.165 RELATIVE A LA PROTECTION DES INFORMATIONS NOMINATIVES

Le message du Président

En 2014, lorsque pour la première fois j'ai eu l'honneur de rédiger le « *Message du Président* », j'avais souligné que les Membres de la CCIN nouvellement nommés et moi-même partagions une vision commune : « *veiller à la protection des informations nominatives avec une réelle volonté de dialogue et de pédagogie envers les responsables de traitements dans un domaine qui s'avère souvent complexe pour eux, sans toutefois faire preuve de la moindre complaisance lorsque des atteintes à la protection des données personnelles sont avérées* ».

L'année 2024 est celle de mon dernier message. En effet quatre mandats de Commissaire sur six, dont le mien, ne pourront plus être renouvelés en vertu des dispositions légales qui limitent à deux périodes quinquennales les fonctions de Membre de la Commission.

L'occasion donc de faire le bilan de notre action ; une action sur 10 ans que l'on peut assimiler, en cette année de Jeux Olympiques, à une sorte de décathlon, épreuve dont je peux dire sans peine, à la veille de quitter mes fonctions de Président de la Commission, que je suis heureux d'y avoir participé. Une action jalonnée d'évènements marquants.

Il a ainsi fallu œuvrer, dès notre prise de fonction, au rétablissement des pouvoirs d'investigations de la CCIN annulés, peu de temps avant notre nomination, par le Tribunal Suprême. Ce fut fait au mois de décembre 2015.

Le 24 mai 2016 a constitué une étape importante avec l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) rendu applicable sur le territoire de l'Union européenne, à compter du 25 mai 2018. C'est en effet à l'aune de ces nouvelles dispositions que sera examiné le caractère adéquat du dispositif de protection des données personnelles de la Principauté.

Il s'agit également d'un texte qui n'est pas sans conséquences pour les responsables de traitements et sous-traitants monégasques. Aussi, en 2017, la Commission a poursuivi ses échanges sur le champ d'application territorial du RGPD et a partagé ses réflexions avec les Autorités de protection des données personnelles de pays tiers à l'Union européenne, mais fortement impactés par ce Règlement du fait de leur proximité géographique avec le territoire européen. En ce sens, elle avait pris part à une démarche commune auprès du Comité européen de la protection des données afin d'obtenir des précisions qui lui ont utilement permis d'apporter des réponses aux nombreuses questions d'entités situées à Monaco et impactées par l'application de ce nouveau cadre normatif européen de portée extraterritoriale.

L'année 2018 a pour sa part été marquée par le début des travaux menés conjointement avec les Services exécutifs de l'Etat, relatifs à la refonte de la législation en matière de protection des données personnelles afin d'y intégrer les grands principes du RGPD ainsi que les modifications apportées à la Convention 108 par le Protocole d'amendement adopté par le Comité des Ministres du Conseil de l'Europe au mois de mai 2018, et signé par les Autorités monégasques dès le 10 octobre de cette même année.

Ces travaux se sont poursuivis en 2019. Cette association précoce a permis à la Commission de faire valoir ses points d'attention spécifiques au regard des standards européens régissant la protection des données personnelles à partir desquels sera évalué le niveau d'adéquation de la Principauté. Notre Commission a cependant pu constater que nombre de ses remarques n'ont pas été prises en compte par le Gouvernement.

La crise sanitaire de 2020 ne fut pas la plus facile des épreuves. Dans ce contexte particulier où la santé des personnes concernées était en jeu, le Gouvernement a adopté des textes visant à gérer les effets de cette pandémie mondiale. Il a également mis en œuvre un traitement d'informations nominatives destiné à permettre le suivi de la situation épidémiologique en Principauté, lequel s'est enrichi de nombreuses données personnelles au fil de l'évolution de la situation sanitaire. Cette crise a toutefois mis en exergue que les enjeux de protection des données personnelles n'étaient pas forcément maitrisés ou priorisés, en attestent les saisines tardives de la Commission sur les projets de texte, voire même l'absence de saisine et de formalités légales, parfois même dans des périodes où l'urgence sanitaire ne pouvait plus être invoquée.

Ainsi, la refonte du cadre monégasque en matière de protection des informations nominatives se faisait encore plus nécessaire et c'est dans ce contexte que la Commission a été saisie sur le projet de Loi relative à la protection des données personnelles, dont l'objectif est d'introduire en droit interne les standards internationaux résultant tout à la fois de la Convention 108+ du Conseil de l'Europe, du RGPD et de la Directive « *Police Justice* ». C'est finalement en décembre 2021, après un second avis de la Commission, que le projet de Loi n° 1054 a été déposé au Conseil National.

Ce projet de Loi n'ayant toujours pas été adopté, l'Autorité de Protection des Données Personnelles (APDP) qu'il crée n'a toujours pas remplacé la CCIN, qui a fêté ses 30 ans le 23 décembre 2023. Le Marathon de l'adéquation initié en 2010 et de l'adoption d'une nouvelle Loi en matière de protection des données personnelles est donc toujours en cours et, comme l'a rappelé le rapport d'activité 2022, nécessitera l'amélioration des pouvoirs de la future APDP afin notamment que la publicité de ses avis soit étendue et que ses sanctions soient proportionnées et dissuasives.

Pour ma part, c'est dans ce contexte et avec espoir que je m'attelle à ma dernière épreuve au sein de la CCIN, le « *passage de relais* ».

Mais avant cela je tiens à remercier chaleureusement les Membres de la Commission qui m'ont apporté leur précieuse contribution et leur soutien tout au long de ces dix années. Mes remerciements les plus sincères vont également aux Agents du Secrétariat Général sans lesquels nous n'aurions pu mener à bien l'ensemble de nos missions.

Guy MAGNAN

Sommaire

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.

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.

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.

En application de l'article 5 de la Loi n° 1.165, l'année 2024 marquera la fin des mandats de 4 des 6 Commissaires de la CCIN, sans possibilité de renouvellement : Messieurs Guy MAGNAN, Rainier BOISSON, Florestan BELLINZONA et Philippe BLANCHI, dont les nominations initiales ont eu lieu à effet du 19 juin 2014. Cette fin de mandat s'effectuera sans préjudice de l'entrée en vigueur éventuelle de la future législation relative à la protection des données personnelles qui prévoit que les membres de la CCIN en exercice à la date de cette entrée en vigueur poursuivent leur mandat en tant que membre de la nouvelle Autorité de Protection des Données Personnelles jusqu'à la nomination des membres de celle-ci.

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

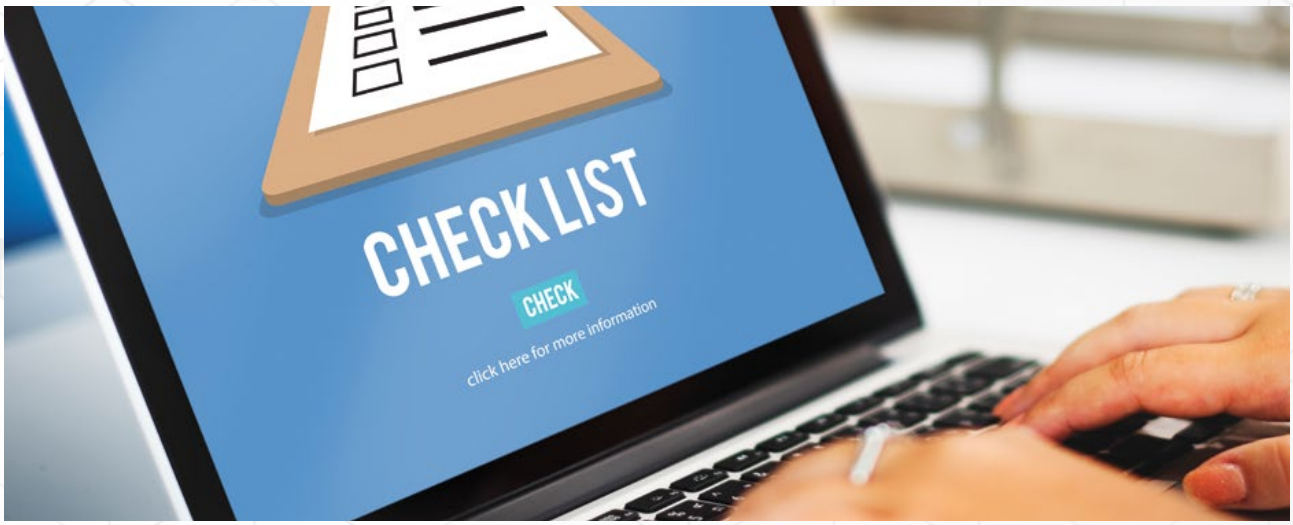
Au travers de la publication :

- 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 ;
- de publications sur sa page LinkedIn.

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 2023 la Commission a été dotée d'un budget total de **1.774.100,00 €**, contre **1.512.300,00 €** en 2022, se répartissant ainsi :
- **1.154.100,00 €** au titre des crédits de fonctionnement, dont plus de la moitié est consacrée au paiement du loyer de ses locaux ;
- **620.000,00 €** au titre de ses dépenses salariales, en augmentation par rapport à l'année précédente. En effet, afin d'anticiper l'évolution de ses missions, la CCIN a demandé une modification de son organigramme dans le but de renforcer ses compétences. Cette modification est intervenue en début d'année 2023.
- Il est à noter que ce montant total inclut la demande faite par la CCIN au titre du budget rectificatif 2023, inhérente à ses changements de locaux, à hauteur de **97.000,00 €**.

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.

Afin d'organiser les Services de la Commission dans la perspective de l'entrée en vigueur de la nouvelle législation relative à la protection des données personnelles, un juriste supplémentaire a rejoint les effectifs en fin d'année 2023. Ce juriste, au profil bien spécifique et spécialisé dans la mesure où il est Magistrat, détaché au sein de la CCIN, a vocation à se charger de l'organisation et du suivi des séances de la future formation restreinte de l'Autorité de Protection des Données Personnelles qui aura en charge le prononcé des sanctions administratives, notamment pécuniaires.

Le Secrétaire Général, le Chargé de Mission, l'informaticien, ainsi que quatre 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.

2 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 2023 ce répertoire a été consulté 3 fois :

- à 2 reprises par des responsables de traitement souhaitant faire le point sur les formalités déjà accomplies, afin de poursuivre leur mise en conformité ;
- une fois par des Délégués du Personnel, afin de vérifier la conformité de leur employeur en matière de traitement des données salariales.

LES PLAINTES

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

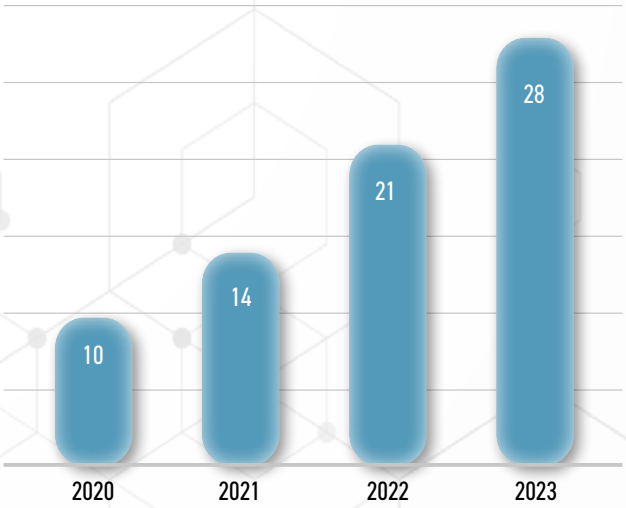
Evolution du nombre total de plaintes adressées à la CCIN depuis 10 ans :

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

Les plaintes liées à l'utilisation des réseaux sociaux

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

Evolution des demandes depuis 2020



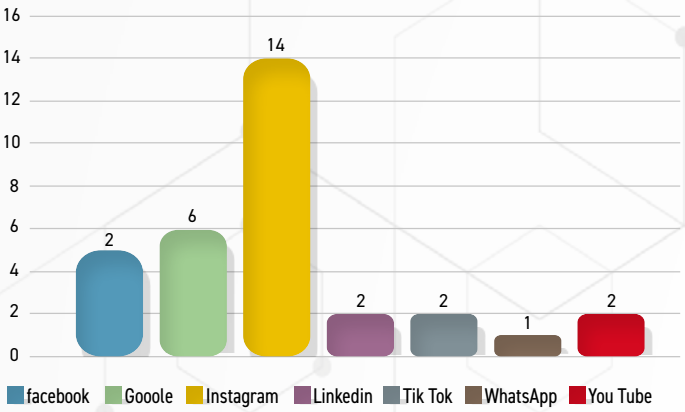
Sur ces 28 plaintes, 2 ont été classées sans suite :

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

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

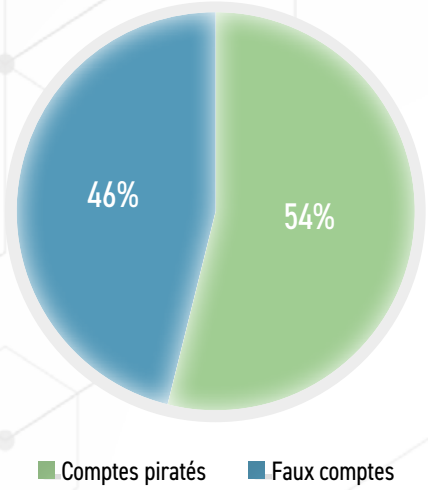
Certaines de ces plaintes concernaient des atteintes à la vie privée sur plusieurs médias.

Médias concernés



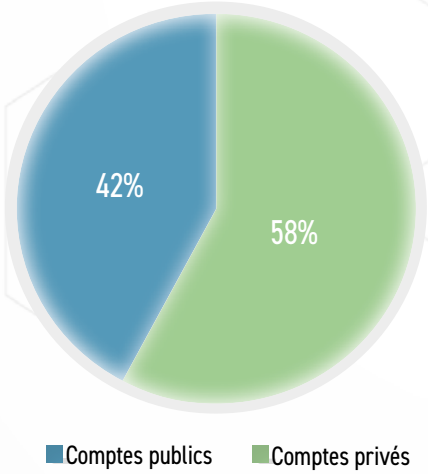
Les demandes ont eu essentiellement pour objet la récupération de comptes piratés (13) et la suppression de faux comptes (11).

Nature des demandes



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

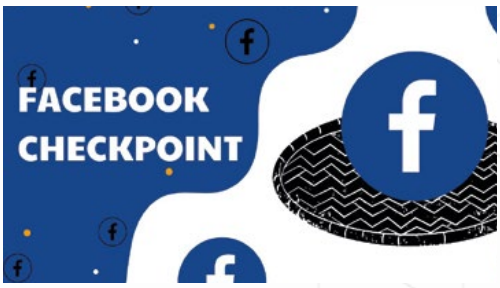
Nature des comptes concernés



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

Ce système empêche les utilisateurs de se connecter à leurs comptes tant qu'ils n'ont pas réalisé une série d'étapes et d'actions. Les checkpoints sont utiles, par exemple, lorsqu'un compte semble être compromis, lorsque plusieurs tentatives de connexion ont échoué ou lorsque les conditions générales et politiques de Meta Platforms Ireland Limited, notamment les politiques en matière d'intégrité et d'authenticité, ont été enfreintes.
Lorsqu'un compte est soumis à un checkpoint, le titulaire de ce compte doit entreprendre des démarches pour faire vérifier son identité afin de récupérer l'accès audit compte et d'éviter que celui-ci ne soit désactivé de manière permanente.

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



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

La CCIN a pu constater une augmentation des demandes de suppression de faux comptes Instagram renvoyant vers des pages à connotation sexuelle. Le profil des victimes est en général toujours le même : des jeunes femmes postant régulièrement des photos d'elles sur leur propre compte Instagram.

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

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

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

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

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

A cet égard, il convient de noter que la plateforme Wix prend très au sérieux ce problème et a mis en place un formulaire, très simple à remplir : wix.com/about/abuse-form

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

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

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

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

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

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

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

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

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

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

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

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

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

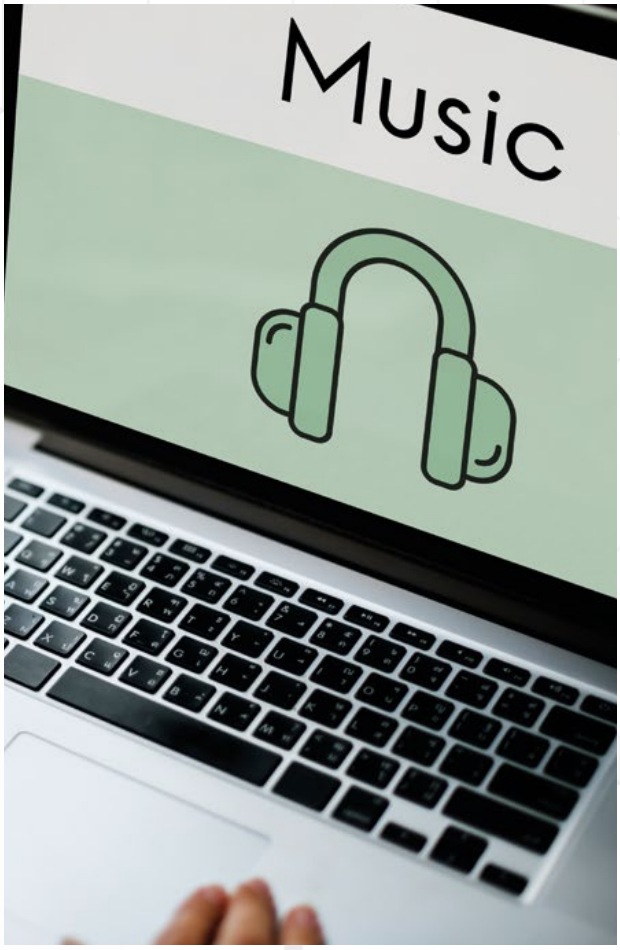
- *une Ordonnance Souveraine prononçant la révocation d'un fonctionnaire ;*
- *plusieurs articles diffusant des propos à caractère diffamatoire concernant des résidents de la Principauté.*

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

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

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

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



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

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

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

Les caméras de vidéosurveillance

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

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

Suite à l'intervention de la CCIN les caméras concernées n'ont pas été installées.

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

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

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

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

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

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

Aussi elle souhaite préciser les bonnes pratiques à adopter.

- *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

[1] Voir infra : les investigations

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

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

Les difficultés en matière d'exercice des droits

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

Des difficultés récurrentes en matière de droit d'accès

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

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

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

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

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

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

La rectification des données transmises à des tiers

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

« *La personne intéressée peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou supprimées les informations la concernant lorsqu'elles*

se sont révélées inexactes, incomplètes, équivoques, périmées ou si leur collecte, leur enregistrement, leur communication ou leur conservation est prohibé.

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

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

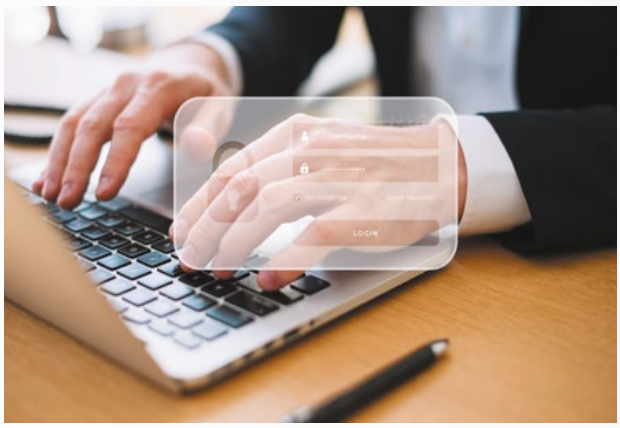
Dans ce cadre la CCIN est intervenue afin qu'un plaignant obtienne la suppression des informations transmises par erreur à un tiers.

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

La désindexation de contenus publiés au Journal Officiel

La CCIN a été saisie à 2 reprises par des personnes ayant fait l'objet de mesures de révocation, publiées au Journal Officiel de Monaco, et non désindexées par le site Internet concerné malgré le nombre d'années écoulées depuis la publication de ces mesures (6 ans pour la plus ancienne). De ce fait les résultats effectués sur les moteurs de recherche à partir de leurs noms faisaient apparaitre ces mesures de révocation, rendant ainsi extrêmement difficiles leurs recherches d'emplois. Face au refus de l'exploitant du site de procéder à cette désindexation, la CCIN a été saisie par les plaignants.

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



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

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

Le traitement des données

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

L'exploitation de sites Internet

Les 2 plaintes reçues en 2023 ont concerné :

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

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

LES INVESTIGATIONS : LES CAMÉRAS DE VIDÉOSURVEILLANCE TOUJOURS AU CENTRE DES ENJEUX DE PRÉSERVATION DE LA VIE PRIVÉE

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

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

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

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

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

La Commission a reçu un signalement en 2023 portant sur l'utilisation d'un système de vidéosurveillance au sein d'un établissement du secteur public.
Aucun avis favorable n'ayant été émis par la Commission pour la mise en œuvre de ce traitement, il a été décidé de procéder à une investigation sur place.
Lors de l'arrivée dans les locaux de l'établissement, les Agents, assermentés, désignés par le Président de la Commission ont constaté que l'un des membres du personnel était en train de filmer, à l'aide d'un téléphone portable, l'écran de contrôle du système de vidéosurveillance.

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

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

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

Conformément aux dispositions de l'article 19 de la Loi n° 1.165 susvisée, un rapport d'investigation a été adressé au responsable des locaux en toute fin d'année 2023 afin de relever les irrégularités à la Loi qui ont été constatées lors des opérations de contrôle. Ce dossier devrait être clôturé en 2024.

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

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

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

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

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

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

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

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

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

Une investigation au sein de plusieurs établissements appartenant à deux sociétés

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

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

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

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

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

L'exploitation de caméras mobiles à des fins de dissuasion

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

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

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

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

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

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

LES SANCTIONS

En 2023 le Président de la CCIN a prononcé 3 avertissements, dont 2 ont été rendus publics au regard des non conformités relevées.

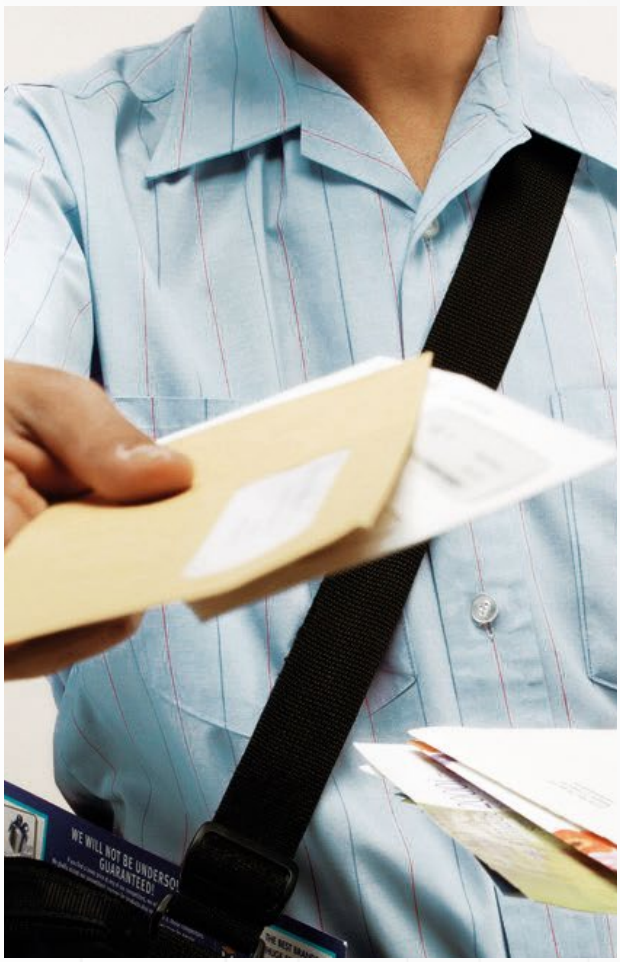
Un avertissement non public pour non-respect du droit d'accès

Le premier avertissement, non public, a fait suite à des échanges intervenus en 2022 avec le responsable de traitement, dans le cadre de l'instruction d'une plainte portant sur un refus de faire droit à une demande de droit d'accès exercé sur le fondement de l'article 15 de la Loi n° 1.165, refus fondé sur les dispositions de 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 relatifs à l'accès aux documents administratifs[2].

Face au refus réitéré de faire droit à cette demande de droit d'accès, le responsable de traitement a fait l'objet d'un avertissement, qui a été l'occasion de lui rappeler :

- la distinction entre le droit d'accès aux données personnelles et l'accès aux documents administratifs ;
- le principe général de non possibilité d'atteinte par un texte réglementaire à un droit légalement conféré ;
- les limites qui auraient pu être apportées à la demande de droit d'accès, et tenant dans le nécessaire respect des droits des tiers (en cela le responsable de traitement avait été invité à procéder à un examen préalable spécifique des informations qu'il détenait et qui pouvaient, ou non être communiquées au demandeur).

Prenant en compte le contexte de cette affaire, et la préoccupation du Service concerné de ne pas porter atteinte aux droits des autres personnes concernées, il a été décidé de ne pas procéder à la publication de cet avertissement.



Afin d'éviter qu'une telle situation se renouvelle, la Commission a appelé de ses vœux à 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.

Deux avertissements publics suite à des contrôles sur place

Les deux avertissements publics ont fait suite à des contrôles effectués en 2022[3].

- Le premier concernait un dispositif de vidéosurveillance implanté dans une station-service, ayant obtenu l'autorisation de mise en œuvre de la CCIN, autorisation toutefois subordonnée au respect de plusieurs demandes. Le contrôle sur place avait permis de constater que les réserves émises par la Commission n'avaient pas été respectées, et que l'exploitation de ce dispositif permettait une surveillance permanente et inopportune des personnes concernées par le biais de l'utilisation

[2] Voir rapport d'activité CCIN 2022 p 21 et suivantes
[3] Voir Rapport d'activité CCIN 2022 p 20, et 26

d'un dispositif d'enregistrement des conversations, expressément exclu pourtant du champ de l'autorisation délivrée par la CCIN.

Lors du contrôle il a également été constaté la rétention de documents d'identité, en dehors de tout cadre légal, lorsque les clients n'étaient pas en mesure de régler sur le champ leurs achats, les privant ainsi de la possibilité de justifier de leur identité, ou de la possession de leur permis de conduire, en cas de contrôle de police.

Au regard des irrégularités qui ont été constatées, et de la gravité de l'atteinte aux droits des personnes soumises à la collecte de leurs conversations au sein de cet établissement, un avertissement public a été adressé au responsable de traitement en fin d'année 2023.

Cet avertissement, publié sur le site Internet de la CCIN et au Journal de Monaco, fera l'objet d'une anonymisation 6 mois après sa publication.

- Le second avertissement public a porté sur l'exploitation non conforme de traitements mis en œuvre dans le cadre de la gestion de la crise sanitaire Covid-19 par les Services de l'Etat.

L'historique de ce dossier, rappelé dans la sanction, a ainsi mis l'accent sur le fait que la CCIN, entre 2020 et 2022, avait, à de nombreuses reprises, alerté le Gouvernement sur la sensibilité des informations nominatives collectées dans le cadre de la gestion de la pandémie, informations dont le quantum n'a cessé de croitre au fil des mois, et sur les mesures qu'il y avait lieu de mettre en œuvre afin d'en limiter les accès.

Les opérations de contrôle sur place ont mis en exergue plusieurs non conformités à la Loi n° 1.165 :

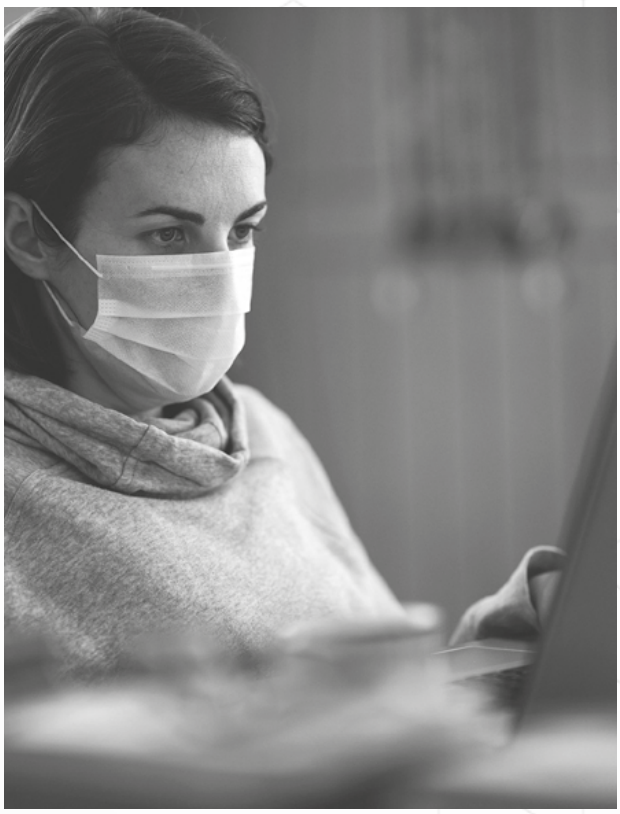
- l'absence de formalités préalables à la mise en œuvre de traitements automatisés d'informations nominatives relatifs à la gestion des cas contacts, au suivi médical des personnes concernées, à l'étude Cordages relative à la viabilité des différentes méthodes de tests et qui comportait tous les antécédents médicaux des participants ;

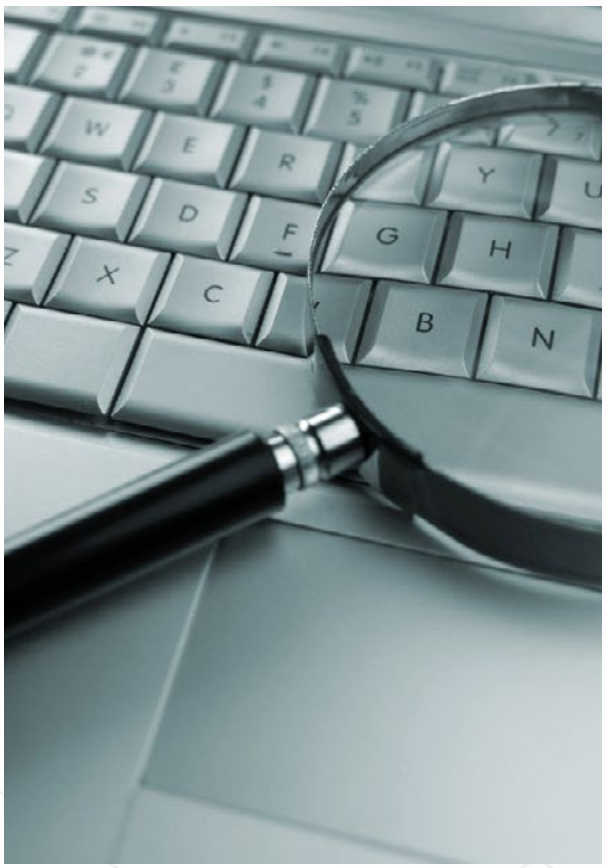
- des durées de conservations excessives et l'absence de mise à jour des données ;

- une information des personnes concernées parfois lacunaire ;

- une sécurité logique et physique non adéquate au regard de la sensibilité des données personnelles traitées.

Eu égard à la sensibilité des données de santé traitées dans le cadre de la crise sanitaire, au nombre de personnes concernées, et au maintien dans la durée de situations non conformes à la législation





applicable, le Président de la CCIN, en accord avec la Commission, a prononcé en fin d'année 2023 un avertissement public à l'encontre du responsable de traitement.

Cet avertissement a été publié au Journal de Monaco et sur le site Internet de la CCIN. Compte tenu du fait que cette sanction peut difficilement être anonymisée, elle sera désindexée du site Internet du Journal de Monaco 2 ans après sa publication.

Sur la publicité des sanctions :

La possibilité de procéder à la publicité des mesures de sanction a été introduite à l'article 19 de la Loi n° 1.165 par la modification législative du 1er décembre 2015.

Si aucune disposition textuelle, et aucune jurisprudence monégasque, ne prévoit des mesures d'anonymisation passé un certain délai, la CCIN a, d'elle-même, décidé de faire procéder à l'anonymisation des sanctions rendues publiques, au maximum 2 ans après leur publication sur son site Internet mais également sur le site Internet du Journal de Monaco. En cela elle prend en considération la décision du Conseil d'Etat français (CE 19/06/2017 n° 396050) précisant qu'une sanction complémentaire de publication d'une décision de sanction « *se trouve nécessairement soumise, et alors même que la loi ne le prévoirait pas expressément, au respect du principe de proportionnalité. La légalité de cette sanction s'apprécie, notamment, au regard du support de diffusion retenu et, le cas échéant, de la durée pendant laquelle cette publication est accessible de façon libre et continue* ». Aussi le Conseil d'Etat français a considéré qu'une mesure de publication d'une sanction sans borne temporelle est excessive.

En revanche l'article 19 de la Loi n° 1.165 prévoit un recours à l'encontre de ces publications : « *Les mesures de publicité peuvent, en cas d'atteinte grave et disproportionnée à la sécurité publique, au respect de la vie privée et familiale ou aux intérêts légitimes des personnes concernées, faire l'objet d'un recours devant le Président du Tribunal de Première Instance, saisi et statuant, comme en matière de référé, aux fins qu'il ordonne la suppression de la publication* ».

3

LES AVIS DE LA COMMISSION SUR LES PROJETS DE TEXTES

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 a été consultée en 2023 à 2 reprises par le Ministre d'Etat, sur 2 projets de Loi.

Une nouvelle fois elle regrette de ne pas avoir été saisie pour avis d'autres projets de textes qui emportent pourtant la collecte de nombreuses

données personnelles, dont notamment les projets d'Ordonnances Souveraines en lien avec la création, ou la modification, de registres en matière de lutte contre le blanchiment de capitaux.

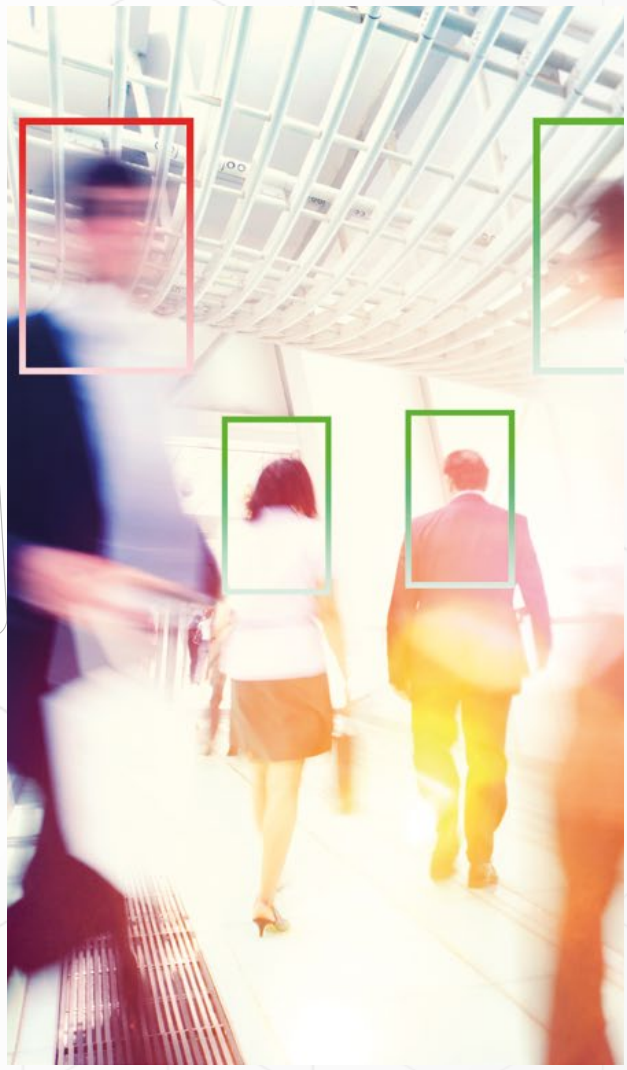
Le projet de Loi relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen d'un système d'identification biométrique à distance

La CCIN a été saisie le 9 février 2023 par le Ministre d'Etat du projet de Loi relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen d'un système d'identification biométrique à distance, lequel vise à introduire en Principauté l'utilisation de la reconnaissance faciale.

Cette saisine fait suite aux échanges entre la CCIN et le Gouvernement intervenus en 2019, et qui avaient conduit le Conseiller de Gouvernement-Ministre de l'Intérieur à déclarer devant le Conseil National, en séance publique du 12 décembre 2019, qu'à la suite de ces échanges le Gouvernement avait convenu de la nécessité de déposer un projet de Loi. En ce sens l'exposé de motifs de ce projet de Loi, accessible sur le site Internet du Conseil National, mentionne que :

> « *[La CCIN] avait très tôt appelé l'attention du Gouvernement Princier sur la nécessité d'engager un débat public quant à l'opportunité et au périmètre de la mise en œuvre de technologies de reconnaissance faciale dans l'espace public pour les finalités de sécurité publique* ».

Aussi la CCIN a rendu son avis au Ministre d'Etat dans la délibération n° 2023-066 du 26 avril 2023. Parmi les nombreuses observations qu'elle a formulées, la Commission a, à titre liminaire, relaté les différents échanges intervenus avec le Gouvernement et le contexte international de la problématique de l'identification à distance d'individus par l'utilisation de solutions d'intelligence artificielle. Le Gouvernement a choisi d'introduire en droit monégasque la reconnaissance faciale par le biais d'une modification de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale. La Commission a regretté que cette modification soit limitée à l'introduction de ce dispositif et qu'il n'y ait pas eu une refonte plus large de ce texte, dont certaines dispositions posent des difficultés notamment au Tribunal Suprême qui a pu relever (Décision TS 2021-10 Mme A. K. c. Etat de Monaco) l'absence de recours juridictionnel effectif qui est pourtant « *inhérent à l'affirmation constitutionnelle de la Principauté de Monaco en tant qu'Etat de droit* » et dont le respect « *participe à la garantie des droits fondamentaux consacrés par le titre III de la Constitution* ». En outre, la Loi n° 1.430 ne permet pas de définir clairement ce qui relève de la vidéosurveillance ou de la vidéoprotection, difficulté renforcée par l'introduction au sein du projet de Loi n° 1.054 relative à la protection des données personnelles, d'une partie dédiée à la vidéosurveillance au contenu proche de ce que le projet de Loi relatif à l'introduction de la reconnaissance faciale propose.



Aussi la CCIN n'a pas manqué de s'interroger sur les interactions entre ces 2 textes, tout en rappelant que selon elle les articles relatifs à la vidéosurveillance n'ont pas leur place au sein du projet de Loi n° 1.054. Elle s'est aussi inquiétée de l'usage éventuel de cette technologie au moyen de drones en sus des caméras de vidéoprotection urbaine, redoutant en effet une certaine assimilation, au sein des Services Gouvernementaux, entre caméras de vidéoprotection et images filmées par les drones, qui à ce jour ne doivent en aucun cas permettre l'identification de personnes.

Les préoccupations de la CCIN se sont également portées sur l'absence de contrôle effectif qui sera opéré sur le dispositif envisagé compte tenu du manque de clarté entre ce qui relève de la sécurité publique, ou de la sécurité nationale qui serait exclue du champ de compétence de la future Autorité de Protection des Données Personnelles (APDP) appelée à lui succéder. Ainsi l'APDP ne pourra connaître des sources de la « *liste d'alerte* » utilisée pour comparer les images de personnes recherchées ou signalées, qui serait alimentée notamment par des traitements mis en œuvre à des fins de sécurité nationale, privant ainsi l'APDP de toute possibilité d'analyser la proportionnalité du dispositif ainsi que l'exactitude et la mise à jour des informations portées sur cette liste.

Un texte réellement limité à la reconnaissance faciale ?

Le projet de Loi ne définit pas « l'identification biométrique à distance », qui peut alors recouvrir d'autres technologies que la seule reconnaissance faciale, comme l'analyse de comportement ou de la température des personnes filmées.

Dès lors, si l'exposé des motifs semble limiter la portée du projet de Loi à l'utilisation de la technologie de reconnaissance faciale, le contenu du dispositif n'emporte pas les mêmes certitudes.

De plus, la Commission s'est étonnée que ce projet n'ait fait l'objet d'aucune analyse de son impact, notamment sur les populations vulnérables objet d'une surveillance accrue, ni du rapport entre ses risques intrinsèques eu égard aux bénéfices attendus.

En effet l'utilisation de cette technologie, dont le risque d'atteinte aux droits fondamentaux des personnes est avéré, s'inscrit dans un contexte où les Etats et organismes étrangers sont encore en réflexion notamment quant aux critères d'absolue nécessité de l'utilisation d'une telle technique que de sa proportionnalité, et où seules certaines expérimentations ont été effectuées.

Pour rappel, les lignes directrices sur la reconnaissance faciale du Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de la Convention 108, à laquelle Monaco est Partie, soulignent notamment que :

« *si elles envisagent le déploiement des technologies de reconnaissance faciale dans des environnements non contrôlés (NB : ouverts au public), les autorités chargées de l'application de la loi devront :*

**évaluer et expliquer dans leur évaluation l'absolue nécessité et la proportionnalité du déploiement de ces technologies ;*

**aborder le risque pour différents droits fondamentaux, notamment pour le droit à la protection des données, à la liberté d'expression, à la liberté de réunion et à la liberté de circulation ou à la lutte contre la discrimination, en fonction des utilisations potentielles en différents endroits* ».

La Commission a par ailleurs relevé que si le projet de Loi prévoit que le dispositif de reconnaissance faciale ne pourra être utilisé que par les Services de la Sûreté Publique, la rédaction en projet peut conduire en réalité à en élargir le champ d'application.

La Commission a également relevé que la notion de lieux accessibles au public telle que prévue comportait une insécurité juridique. Elle a souhaité que soit mieux encadré le régime de transmission des images capturées par des dispositifs de vidéosurveillance privés, à la Direction de la Sûreté Publique.

Elle a également mis en exergue les difficultés d'application entre le régime de l'identification biométrique à distance en temps réel et celui de l'identification en temps différé. Elle a souligné en outre que si le Gouvernement faisait état de la volonté de ne procéder à l'identification biométrique à distance que des personnes soupçonnées de faits d'une gravité certaine, le fait de soumettre au dispositif toute personne encourant un an seulement d'emprisonnement permettrait un recours extensif à cette technologie. Elle s'est de plus inquiétée, dans certains cas, de la possibilité de remonter d'une personne à une autre engendrant en recours extensif au système.

Enfin, elle s'est étonnée de ce que les peines encourues en cas d'infraction aux prescriptions légales en la matière soient moins lourdes que celles concernant les infractions aux dispositions relatives aux informations nominatives dans la Loi n° 1.165 et qu'aucune infraction ne soit prévue en cas d'usage indu du dispositif par un agent de la Sûreté Publique.

En date du 19 décembre 2023, le projet de Loi a été déposé sur le bureau du Conseil National. Si le texte a un peu évolué, il est regrettable que les changements soient mineurs et uniquement limités à éviter des impasses techniques ou pratiques mises en exergue dans l'avis de la CCIN. En effet, aucune modification de fond de nature à répondre aux risques identifiés sur les droits et libertés fondamentaux des personnes concernées n'a été apportée. La Commission regrette ainsi le peu d'écho donné à ses remarques, alors que l'exposé des motifs de ce projet de Loi mentionne qu'« *A cet égard, les autorités administratives et judiciaires sont particulièrement attentives aux avis et recommandations de la C.C.I.N., témoignant d'un attachement commun des acteurs concernés quant à la préservation des droits et libertés fondamentaux dans le domaine des nouvelles technologies de la communication et de l'information, attachement sur lequel reposent la coopération et le dialogue entre l'autorité de protection des données et les services administratifs et judiciaires* ».

Aussi la CCIN déplore que cette affirmation ne se soit traduite, au sein de ce projet de Loi pourtant porteur d'enjeux d'importance en matière de préservation des droits et libertés fondamentaux, que par un effet d'annonce non concrétisé au sein du dispositif, et redoute ainsi que le texte projeté ne soit pas conforme aux standards européens minimums, que cela résulte d'une réelle volonté ou d'une incompréhension.

Sans se positionner sur l'opportunité d'introduire un tel dispositif biométrique, qui est du ressort des co-législateurs, la CCIN rappelle qu'en tout état de cause, les droits et libertés fondamentaux des personnes concernées doivent être garantis. Il convient d'appeler l'attention, sans être exhaustif, sur des éléments essentiels à prévoir dont :

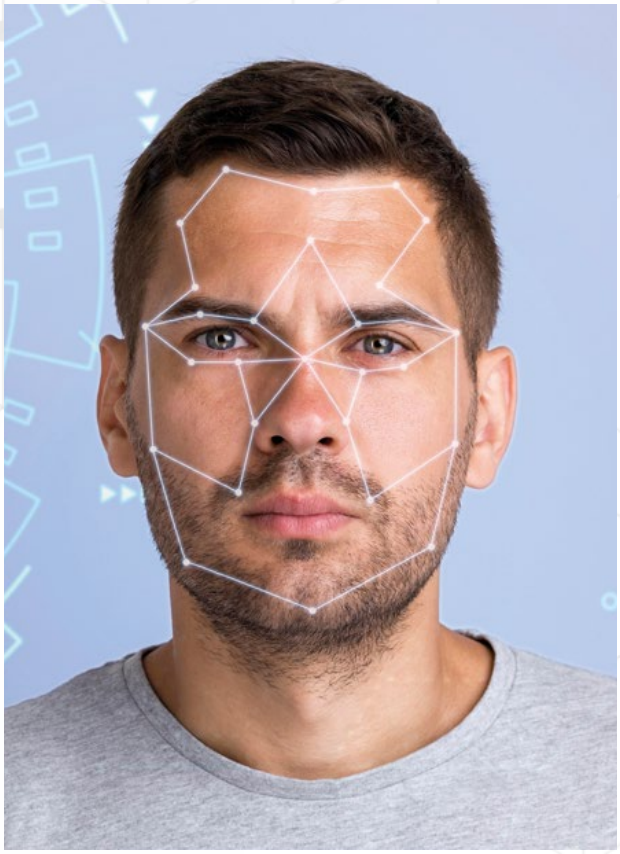
- Une étude du rapport entre le bénéficie sécuritaire attendu eu égard aux potentielles atteintes aux droits et libertés fondamentaux ;

- Une obligation d'analyser les mécanismes d'apprentissage de reconnaissance des visages du logiciel et de parer d'éventuels biais ;

- Une étude sur l'impact du dispositif sur les personnes vulnérables, notamment celles « *qui ne jouissent pas de la plénitude de leurs facultés mentales* » qui semblent pouvoir être soumises à ce dispositif biométrique ;

- L'explication claire des traitements sources qui permettent d'établir les listes de personnes soumises à ce dispositif ;

- L'introduction de définitions.



Le projet de Loi relative à la protection des personnes se prêtant à la recherche

Ce projet de Loi a pour vocation première d'adopter une classification des recherches impliquant la personne humaine qui ne se fonderait plus, comme tel est actuellement le cas en application de la Loi n° 1.265 du 23 décembre 2002 relative à la protection des personnes dans la recherche biomédicale, sur la distinction entre les recherches avec, ou sans, bénéfice individuel direct pour les personnes qui s'y prêtent.

Par délibération n° 2023-067 du 26 avril 2023 la Commission a émis un avis sur ce projet de Loi en mettant en perspective les dispositions objet de ce projet de texte, avec celles prévues dans le projet de Loi n° 1.054 relative à la protection des données personnelles, qui a vocation à encadrer le traitement des données de santé notamment en matière de recherches.

Ceci a conduit la Commission à analyser les modalités prévues en matière d'expression du consentement à la participation à des recherches interventionnelles, en souhaitant que la manifestation écrite du consentement soit en définitive prévue dans le projet de Loi sur les recherches.

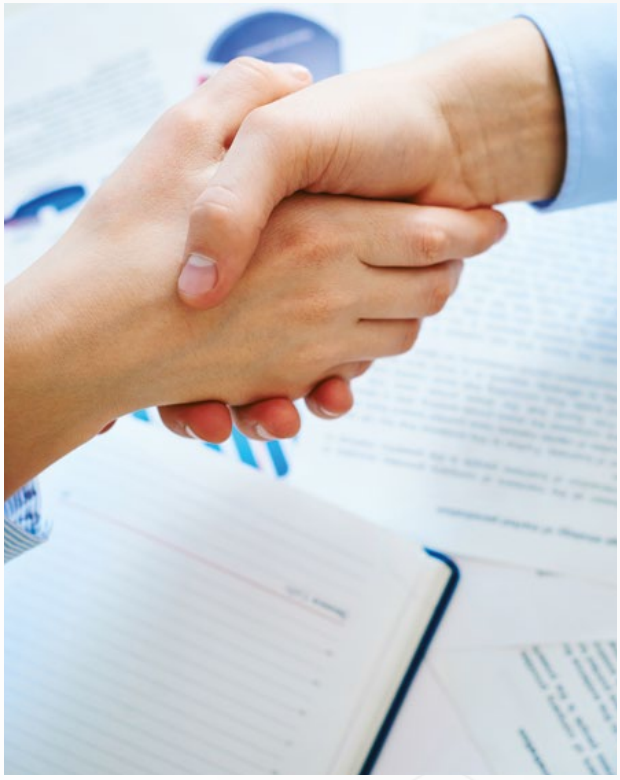
Si ces recherches prévoient une possibilité d'utilisation des données personnelles pour des recherches ultérieures, il conviendrait alors que l'expression du consentement soit spécifique et s'effectue finalité par finalité, afin de permettre aux participants de garder le contrôle sur l'utilisation de leurs données. Aussi la Commission a recommandé une expression du consentement par le biais de cases à cocher pour chaque finalité distincte afin de se prémunir contre l'utilisation des données personnelles à des fins éloignées des finalités initiales, permettant ainsi d'éviter une utilisation détournée desdites données.

Elle a également porté une attention particulière à l'information préalable des personnes concernées :

- concernant les modalités de retrait de leur consentement : en effet la Commission a souligné qu'il doit être aussi simple de retirer son consentement que de le donner, et que l'expression de l'opposition doit également pouvoir s'effectuer aussi facilement que la non opposition, ce qui suppose une information préalable exhaustive et précise sur ce point ;

- lorsqu'elles retirent leur consentement, ou manifestent leur opposition après le début de la recherche, afin que les conséquences de cette décision soient connues d'elles avant leur participation, considérant en effet indispensable que les participants à une recherche soient préalablement informés du devenir de leurs données en cas de retrait de l'étude.

La Commission a par ailleurs relevé que les futures recherches seraient soumises à des régimes différents selon leur typologie (recherche interventionnelle de catégorie 1, ou de catégorie 2, et recherche non interventionnelle), leur mise en œuvre devant faire l'objet d'une autorisation ou d'une déclaration auprès de l'Autorité compétente dont la désignation se fera par un Arrêté Ministériel. De même certaines recherches seront soumises à l'avis préalable du Comité de protection des personnes se prêtant à la recherche. Ces éléments ont conduit la CCIN d'une part, à souhaiter qu'il soit mentionné que l'avis dudit



Comité doit être favorable dans tous les cas et que les déclarations fassent l'objet de la délivrance d'un récépissé, et d'autre part, qu'il soit fait obligation de transmettre à la CCIN, ou à l'APDP appelée à lui succéder, les avis rendus par ce Comité, ainsi que les autorisations ou les déclarations / récépissés délivrés. En effet ces éléments lui permettront de s'assurer de la légalité des recherches qui lui seront soumises pour avis.

Elle a en outre relevé que le texte en projet fait référence à la « *méthodologie de la recherche au regard de la loi n° 1.165* », s'inspirant ainsi des dispositions françaises qui prévoient la compétence de la CNIL pour établir ces méthodologies. Cependant ni l'actuelle Loi n° 1.165, ni la future législation relative à la protection des données personnelles, confèrent une telle possibilité à la CCIN / APDP. Aussi la Commission a estimé qu'il devrait être inséré dans le Loi relative aux recherches médicales, la prise en compte des recommandations de la CCIN / APDP.

Enfin la CCIN a mentionné les modifications qu'il y a lieu d'apporter à l'actuelle Loi n° 1.165 afin de la mettre en cohérence avec le texte en projet, si celui-ci devrait entrer en vigueur rapidement, ainsi que toutes les modifications à apporter au projet de Loi n° 1.054, susmentionné, là aussi dans un souci de cohérence.

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

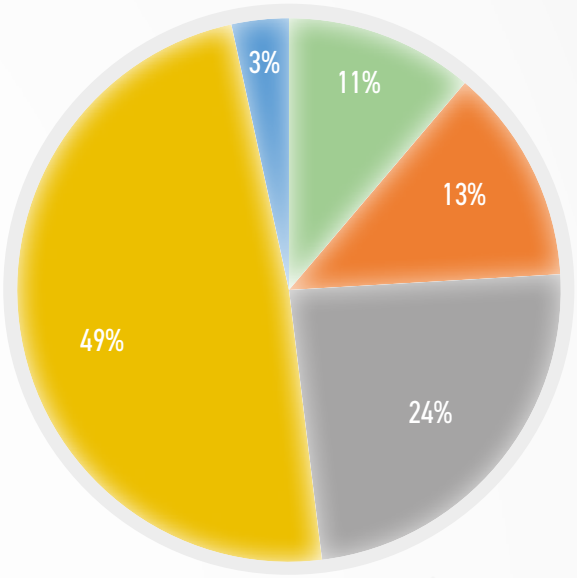
concernent la sécurité publique, les infractions, les condamnations ou les mesures de sûreté, ou ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

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

7.468 *se répartissant ainsi :*

- ***837*** traitements du secteur public ou assimilé ;
- ***961*** traitements ayant fait l'objet d'une autorisation de la Commission ;
- ***1.791*** traitements ayant fait l'objet d'une déclaration ordinaire ;
- ***3.625*** traitements ayant fait l'objet d'une déclaration simplifiée ;
- ***254*** autorisations de transfert vers un Pays ne disposant pas d'un niveau de protection adéquat

Répartition du total des traitements inscrits au répertoire public



Nombre de traitements inscrits annuellement au répertoire par typologie :

Autorisation : DAUT ; Avis : DA ; Déclaration : DO ; Déclaration simplifiée : DS

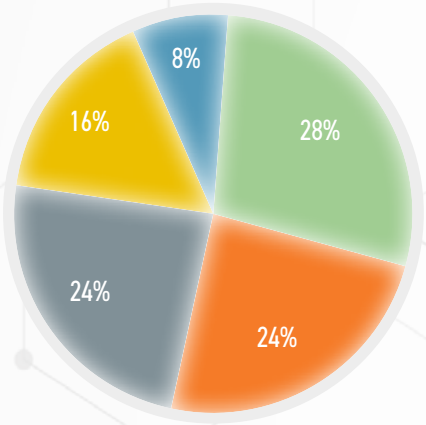
	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
DS		26	26	68	21	16	45	46	19	54	856	144	86	180	201	162	221	243	326	188	177	206	227	87
DO	5	20	20	75	51	60	55	82	42	56	51	32	79	55	121	115	81	140	141	98	82	136	117	77
DA	6	22	22	13	17	11	2	12	16	4	22	38	71	68	67	23	34	38	54	35	66	88	56	52
DAUT								1		1	7	38	38	31	87	62	89	119	90	97	72	91	64	74
TRANSFERT														1	1	4	21	21	41	29	26	54	32	24

Nombre de délibérations rendues par la Commission en 2023 :

Au cours de l'année écoulée, la Commission a rendu **201** délibérations se répartissant comme suit :

- **92** autorisant la mise en œuvre ou la modification de traitements
- **71** portant avis favorable à la mise en œuvre ou à la modification de traitements
- **24** 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
- **5** portant sur une mission d'investigation
- **4** portant refus d'autorisation
- **1** portant refus d'autorisation de transfert
- **1** portant avis défavorable
- **1** portant sur les délais de conservation d'une déclaration ordinaire

REPARTITION DES NOUVEAUX TRAITEMENTS INSCRITS EN 2023



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

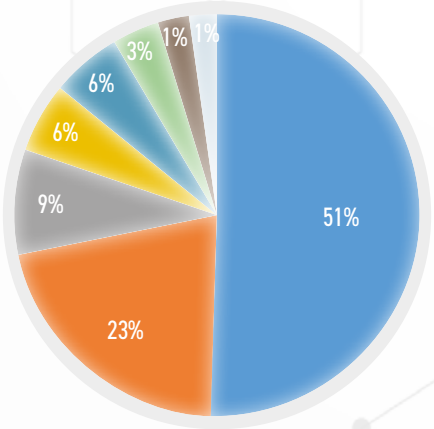
Nombre de nouveaux traitements inscrits au répertoire en 2023 :

314 traitements ont été inscrits en 2023 au répertoire public, se répartissant comme suit :

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

LES TRAITEMENTS DU SECTEUR PUBLIC

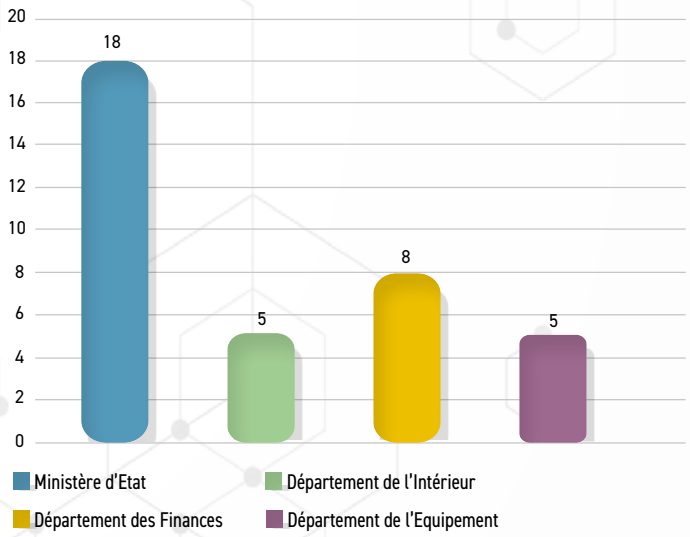
Avis favorables rendus en 2023



- Etat de Monaco
- SMEG
- Commune
- CHPG
- Conseil National
- CAR
- Monaco télécom
- CCIN

La moitié des avis favorables rendus par la Commission en 2023 a concerné des traitements soumis par les services de l'Etat.

Les Départements de l'Etat concernés



La refonte des sites Internet du Gouvernement

Afin de garantir aux utilisateurs une meilleure qualité de navigation et d'accès à l'information, sur tous types de support, le Gouvernement a souhaité procéder à la refonte de ses sites Internet.

Conformément aux dispositions de l'article 7 de la Loi n° 1.165 du 23 décembre 1993, modifiée, la Commission a rendu 3 avis favorables à la mise en œuvre des traitements ayant pour finalités :

- « *Gestion des sites Internet du Gouvernement Princier de Monaco* » (délibération n° 2023-062 du 19 avril 2023) ;
- « *Gestion du site Internet Legimonaco* » (délibération n° 2023-089 du 21 juin 2023) ;
- « *Gestion du site Internet Gel de Fonds* » (délibération n° 2023-180 du 15 novembre 2023).

S'agissant du traitement ayant pour finalité « Gestion des sites Internet du Gouvernement Princier de Monaco »

Parmi les fonctionnalités déployées dans le cadre de ce traitement, il a été constaté la mise à disposition d'un formulaire de contact permettant aux administrés d'entrer électroniquement en contact avec les entités de l'Administration.

La Commission a, à cet égard, pris acte que des demandes d'avis distinctes lui seraient adressées en cas d'utilisation spécifique de formulaires ou en cas de traitement de données sensibles.

Le responsable de traitement a notamment précisé dans le cadre de sa demande d'avis que « *les formulaires de contact et de participation à une activité ou de demande de rappel « sont accessibles uniquement après le consentement de l'intéressé* » ».

Eu égard au quantum des informations pouvant être collectées par le biais de ces formulaires (ex identité de l'internaute, adresse et coordonnées, ID de la demande enregistrée en back-office, type de requête et message de l'internaute), la Commission a été interpellée par la durée de conservation de 5 ans à compter de la demande retenue par le responsable de traitement.

Elle a, à cet égard, considéré que ces données devraient être conservées, le temps du traitement de la demande, par le personnel de l'Administration du Service métier concerné ou, en lien avec la finalité du formulaire contact, par exemple, 3 ans pour l'exercice d'un droit d'accès et a fixé en conséquence la durée de conservation.

S'agissant du traitement ayant pour finalité « Gestion du site Internet Legimonaco »

La Commission s'est associée aux propos du Ministre d'Etat pour qui « *Il est essentiel de rendre le droit accessible à toutes et tous car il régit naturellement notre vie quotidienne. Grâce aux crédits nécessaires votés par le Conseil National, le Gouvernement Princier entend proposer un outil numérique de dernière génération qui offrira un moteur de recherche très performant, de nouveaux contenus et des fonctionnalités enrichies par rapport à la version actuelle, afin de mieux répondre aux besoins des professionnels du droit comme du grand public* ».

Elle a toutefois attiré l'attention du responsable de traitement sur le fait que certains textes règlementaires liés à des traitements de Police ne sont pas accessibles sur cet outil.

Par ailleurs, le responsable de traitement a renseigné, au titre d'une des fonctionnalités de ce traitement, la mise à disposition d'un formulaire permettant de contacter la Direction des Affaires Juridiques.

Il a été indiqué que la mise à disposition de ces formulaires résulte d'une interconnexion avec le traitement relatif à la « *Gestion des sites internet du Gouvernement Princier de Monaco* ». Ainsi, il a été précisé que les informations relatives au formulaire de contact étaient conservées 5 ans dans le back-office du traitement « *Gestion des sites internet du Gouvernement Princier de Monaco* ».

Aussi, dans le prolongement de sa délibération n° 2023-062 relative audit traitement, la Commission a, de nouveau, fixé la durée de conservation de ces informations au temps du traitement de la demande par le personnel de l'Administration du Service métier concerné, ou en lien avec la finalité du formulaire contact, par exemple 3 ans pour l'exercice d'un droit d'accès.

S'agissant du traitement ayant pour finalité « Gestion du site Internet Gel de Fonds »

Enfin, la Direction du Budget et du Trésor (DBT) a souhaité se doter d'un site Internet dédié afin de procéder à la diffusion des informations relatives au gel de fonds et de ressources économiques et mettre à la disposition des internautes une documentation leur permettant d'acquérir une meilleure compréhension de la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Parmi les fonctionnalités associées à ce traitement, il a été renseigné l'existence d'un formulaire de contact et d'une lettre d'informations notifiant aux assujettis les modifications apportées à la liste nationale des Gels de Fonds.

S'agissant du formulaire de contact, il a, de nouveau, été constaté que la gestion de ce dernier s'effectuait par le biais d'une interconnexion avec le traitement ayant pour finalité « *Gestion des sites du Gouvernement Princier de Monaco* ».

Par ailleurs, il a été précisé que la diffusion des lettres d'informations aux personnes qui y souscrivent s'effectue par l'intermédiaire d'un traitement ayant pour finalité « *Gestion des communications internes et externes du Gouvernement Princier* ». Ce dernier n'ayant fait l'objet d'aucune formalité auprès d'elle, la Commission a rappelé que toute interconnexion ne peut avoir lieu qu'entre des traitements légalement mis en œuvre. Partant, elle a demandé que ce traitement lui soit soumis dans les plus brefs délais.

En toute fin, la Commission a pris acte de l'initiation, par les services de l'Etat, de travaux techniques afin de permettre au responsable de traitement de se conformer à la durée de conservation fixée, dans le cadre de ses délibérations, s'agissant des formulaires de contact. Des discussions sont actuellement en cours avec la CCIN sur ce point.

Les traitements du Conseil National

Le Conseil National a continué en 2023 sa mise en conformité avec la Loi n° 1.165 du 23 décembre 1993, modifiée, en soumettant à la Commission 4 nouveaux traitements.

Ainsi, par délibération n° 2023-014 du 15 février 2023, elle a émis un avis favorable à un traitement ayant pour finalité « *Gestion des informations des Conseillères Nationales et des Conseillers Nationaux* ».

Ce traitement « *permet de recueillir des données nécessaires au bon fonctionnement du Conseil National et des relations entre les diverses Institutions de l'Etat, ainsi que la bonne réalisation des missions des conseillères nationales et des conseillers nationaux, telles que :*

- le travail législatif ;

- les représentations officielles et protocolaires ;

- les manifestations audiovisuelles ;

- les règles de fonctionnement de la déontologie. »

Les données collectées sont soit des informations publiques soit des informations fournies par les personnes elles-mêmes par le biais d'une fiche de présentation qu'elles remplissent.

Ces données sont conservées une année après la fin de la mandature, à l'exception des informations relatives à l'identité et à la vie publique des élus qui sont conservées à des fins historiques et de leurs coordonnées internes qui ne sont conservées que le temps de leur mandat.

Des communications de certaines données pouvant être effectuées à destination, entre autres, de la Trésorerie Générale des Finances en sa qualité

de payeur général de l'Etat, la Commission a toutefois demandé que ces communications soient sécurisées en tenant compte de la nature des informations transmises.

Le 19 juillet 2023, la Commission a émis un avis favorable à la mise en œuvre du traitement ayant pour finalité « *Gestion de la messagerie professionnelle du Conseil Nationa*l », sous réserve que les informations liées aux messages (fichiers journaux) ne soient conservées qu'un an.

Lors de la même séance, le traitement ayant pour finalité « *Gestion de la vidéosurveillance du Conseil National* » a lui aussi fait l'objet d'un avis favorable. La Commission a néanmoins rappelé que les caméras mobiles, après mouvement de l'objectif, ne devaient pas filmer les postes de travail des salariés, les lieux privatifs mis à leur disposition, ainsi que la voie publique.

Enfin, par délibération n° 2023-117 du 20 septembre 2023, la Commission s'est prononcée favorablement à la mise en œuvre du traitement ayant pour finalité « *Gestion du contrôle des accès au bâtiment du Conseil National par badge magnétique et digicode* » en rappelant toutefois que les documents d'information devaient impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

Les traitements dans le domaine de la santé

Les traitements liés au fonctionnement du CHPG

En 2023, le Centre Hospitalier Princesse Grace (CHPG) a soumis à la Commission deux nouveaux traitements pour avis.

Le premier d'entre eux concernait la « *Gestion des admissions des étudiants en Institut de Formation en Soins Infirmiers et en Institut de Formation d'Aides-Soignants* » qui a fait l'objet d'un avis favorable par délibération n° 2023-103 du 19 juillet 2023, sous réserve que l'extrait du casier judiciaire soit supprimé dès vérification.

Le 20 septembre 2023, la Commission s'est également prononcée favorablement à la mise en œuvre par le CHPG d'un traitement ayant pour finalité « *Portail patient du CHPG* ». Celui-ci a vocation à faciliter la prise en charge du patient par la création automatique de son espace (accès centralisé à ses informations) lui permettant entre autres de gérer ses rendez-vous et de payer en ligne ses factures.

Pour ces deux traitements, la Commission a néanmoins 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, en cas de doute, que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Elle a également rappelé que l'information préalable des personnes concernées doit impérativement être conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Les recherches médicales

Le CHPG a également soumis 9 recherches médicales à la Commission pour avis, soit en tant que responsable de traitement, soit en tant que représentant d'un promoteur situé en dehors de la Principauté. Parmi ces recherches, 5 étaient des études biomédicales et 4 des études observationnelles.

Les remarques de la Commission pour cette année se résument comme suit :

Sur les données collectées :

- les informations relatives à la race et l'origine ethnique ne doivent pas être collectées en Principauté, ces données ne pouvant être recueillies que lorsque la nature de la recherche le justifie ;

- les commentaires figurant sur le document non automatisé tenu par le médecin investigateur permettant, si nécessaire, l'identification du sujet, doivent être factuels et ne pas comporter d'appréciations pouvant revêtir un caractère insultant ou discriminant.

Sur les documents d'information (note d'information et formulaire de consentement) :

- les documents d'information doivent informer les patients qu'en cas de retrait de leur consentement, leurs données personnelles pourraient ne pas être supprimées si cela devait rendre impossible ou compromettre la réalisation de la recherche ;

- lesdits documents doivent également mentionner tout transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat ou tout accès aux données par du personnel/des prestataires se situant dans des pays ne disposant pas d'un tel niveau de protection.

Sur la sécurité des traitements :

- toute base de données archivée doit être chiffrée sur son support de réception ;

- si des prestataires techniques devaient avoir accès au traitement, leurs droits d'accès devront être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, et ils seront soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de l'article 17 de la Loi n° 1.165 du 23 décembre 1993 ;

- les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises ;

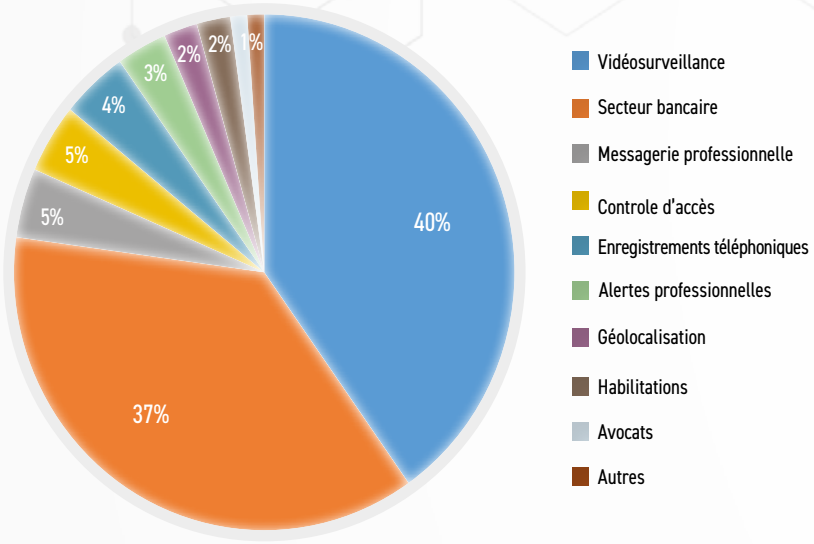
- si un médecin ou un Attaché de Recherche Clinique (ARC) devait rejoindre la recherche après son début, l'identifiant et le mot de passe doivent lui être communiqués par deux canaux distincts.

encore des avocats pour les activités en lien avec les transactions financières ou immobilières de leurs clients[4] .

LES TRAITEMENTS DU SECTEUR PRIVÉ : FOCUS SUR DES PROBLÉMATIQUES SPÉCIFIQUES

Dans le cadre de l'examen des traitements mis en œuvre en matière de LAB-FT-C, la Commission est très souvent amenée à rappeler, et à demander, que les dispositions légales et réglementaires régissant ce domaine très technique, soient strictement respectées, afin de ne pas étendre le champ d'application et la portée des mesures de vigilance légalement prévues.

Autorisations délivrées en 2023



Les traitements mis en œuvre en matière de lutte contre le blanchiment de capitaux

En 2023 la Commission a rendu 18 délibérations relatives à la lutte contre le blanchiment de capitaux, le financement du terrorisme, la prolifération des armes de destruction massive et la corruption (LAB-FT-C).

Si l'essentiel de ces délibérations a concerné des établissements bancaires et assimilés, certaines d'entre elles ont porté sur d'autres catégories d'entités assujetties à la Loi n° 1.362, modifiée, comme par exemple des experts comptables, des loueurs de navires, ou

Ainsi, si **la finalité** du traitement choisie par le responsable de traitement n'appelle généralement pas d'observation de sa part dans la mesure où elle est précise et explicite (ex : « *Gestion de l'identification/vérification des personnes soumises à la Loi relative à la lutte contre le blanchiment de capitaux– KYC* »- ; « *Répondre aux demandes de renseignements du SICCFIN / AMSF* » ou « *Gestion des déclarations de soupçon* »), **le périmètre** des mesures de vigilance fait fréquemment l'objet de remarques de la part de la CCIN. Elle est ainsi souvent amenée à rappeler que les salariés des entités assujetties ne peuvent être concernés par le traitement qu'en tant que gestionnaires des opérations et qu'ils ne doivent pas faire l'objet des mesures de vigilance mises en place dans le cadre de ces traitements.

En effet, et pour rappel, s'agissant des salariés de ces entités, l'article 30 de l'Ordonnance Souveraine n° 2.318, modifiée, portant application de la Loi n° 1.362, modifiée, vient préciser que les risques au regard de la lutte contre le blanchiment de capitaux et le financement du terrorisme doivent être pris en compte dans le recrutement du personnel, et selon le niveau des responsabilités exercées.

[4] Pour les traitements LAB des Avocats voir Rapport d'activité CCIN 2021 p 96

S'agissant des vérifications relatives aux personnes politiquement exposées, là encore la CCIN rappelle fréquemment que la liste des personnes revêtant cette qualification est expressément et limitativement prévue par l'article 24 de l'Ordonnance Souveraine n° 2.318, cet article listant également les personnes réputées membres de leur famille, à savoir :

« *1°) le conjoint ou la personne vivant maritalement avec une personne politiquement exposée ;*

2°) le partenaire lié par un contrat de vie commune ou par un contrat de partenariat enregistré en vertu d'une loi étrangère ;

3°) les ascendants ou descendants directs d'une personne politiquement exposée ainsi que leur conjoint ou leur partenaire lié par un contrat de vie commune ou par un contrat de partenariat enregistré en vertu d'une loi étrangère. »

Tel est également le cas des personnes étroitement associées aux personnes politiquement exposées, dont le périmètre précis est défini audit article, et qui ne concerne pas « *toutes personnes d'intérêt* », notion très large aux contours incertains parfois employée par les responsables de traitement dans les demandes d'autorisation soumises à la CCIN.

« *La Commission rappelle que seules les personnes expressément visées par la Loi n° 1.362 du 3 août 2009, modifiée et ses textes d'application sont susceptibles d'être l'objet des diligences qui s'y rapportent et demande donc au responsable de traitement de s'y conformer.* »

Si la CCIN porte une attention particulière à une application stricte, et conforme aux textes régissant le domaine, du périmètre des personnes soumises aux mesures de vigilance, elle est également amenée à relever que parfois les responsables de traitement omettent certaines catégories d'entre elles. Aussi les délibérations de la Commission « *réintègrent* » lesdites catégories afin de ne pas mettre les entités assujetties en situation de risque juridique.

Par ailleurs la CCIN constate fréquemment que, si **les catégories d'informations** traitées en matière de LAB-FT-C ne posent généralement pas de difficulté, **l'origine des informations** appelle de sa part des remarques, en ce que les responsables de traitement mentionnent très souvent faire des recherches sur Internet afin de remplir leurs obligations de vigilance, et compléter la documentation KYC sur les prospects ou leurs clients.

Ce constat l'amène à rappeler que l'article 3 de la Loi n° 1.362, modifiée, précise que pour l'identification et l'évaluation des risques de blanchiment de capitaux, de financement du terrorisme et de corruption, il doit être tenu compte :

- « *des facteurs inhérents aux clients, aux produits, services, canaux de distribution, du développement de nouveaux produits et de nouvelles pratiques commerciales, y compris les nouveaux mécanismes de distribution et l'utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou les produits préexistants ainsi qu'aux pays ou zones géographiques ;*
- *des documents, recommandations ou déclarations émanant de sources fiables, comme les organismes internationaux spécialisés dans la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive et la corruption ;*
- *de l'évaluation nationale des risques ; et*
- *des lignes directrices établies, selon les cas, par l'Autorité monégasque de sécurité financière ou par le Conseil de l'Ordre des avocats-défenseurs et des avocats.* »

Ainsi les recherches Internet ne sauraient constituer des « *sources fiables* ».

Ces mêmes dispositions sont également rappelées en matière **de profil d'évaluation des risques**, lorsqu'il

est mentionné dans les demandes d'autorisation soumises à la CCIN que ledit profil est calculé de manière automatique par les outils utilisés par le responsable de traitement.

Cette mention la conduit également à demander à ce que le traitement qui lui est soumis respecte les dispositions de l'article 14-1 de la Loi n° 1.165, modifiée, aux termes duquel :

« *Toute personne a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé d'informations destiné à définir son profil ou à évaluer certains aspects de sa personnalité.*

Une personne peut toutefois être soumise à une décision mentionnée au précédent alinéa si cette décision :

- est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue et de voir réexaminer sa demande, garantissent la sauvegarde de son intérêt légitime ;

- ou est autorisée par des dispositions légales ou réglementaires qui précisent les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée ».

Le domaine qui appelle le plus souvent, de manière quasi régulière, des remarques et des demandes de la Commission concerne **les durées de conservation** des informations traitées en matière de LAB-FT-C, pour lesquelles les entités assujetties à la Loi n° 1.362, modifiée, mentionnent fréquemment un délai de conservation de 5 ans à compter de la fin de la relation d'affaires, et ce quelle que soit la nature des informations.

Pourtant, la Loi n° 1.362, modifiée, prévoit expressément certaines durées de conservation, que ce soit en matière connaissance de la clientèle, de vérification des opérations, ou concernant les prospects :

Article 23 de la Loi n° 1.362 :

« *Les organismes et les personnes visés aux articles premier et 2 sont tenus de conserver pendant une durée de cinq ans :*

- *après avoir mis fin aux relations avec leurs clients habituels ou occasionnels, une copie de tous les documents et informations, quel qu'en soit le support, obtenus dans le cadre des mesures de vigilance relatives à la clientèle, notamment ceux qui ont servi à l'identification et à la vérification de l'identité de leurs clients habituels ou occasionnels ;*

- *à partir de l'exécution des opérations, les documents et informations, quel qu'en soit le support, relatifs aux opérations faites par leurs clients habituels ou occasionnels, et notamment une copie des enregistrements, des livres de comptes, de la*

correspondance commerciale de façon à pouvoir reconstituer précisément lesdites opérations ;

- *une copie de tout document en leur possession remis par des personnes avec lesquelles une relation d'affaires n'a pu être établie, quelles qu'en soient les raisons, ainsi que toute information les concernant.*

Le délai de conservation susmentionné peut être prorogé pour une durée supplémentaire maximale de cinq ans :

1°) à l'initiative des organismes et des personnes visés aux articles premier et 2 lorsque cela est nécessaire pour prévenir ou détecter des actes de blanchiment de capitaux ou de financement du terrorisme et de la prolifération des armes de destruction massive sous réserve d'une évaluation au cas par cas de la proportionnalité de cette mesure de prolongation ;

2°) à la demande de l'Autorité monégasque de sécurité financière ;

3°) à la demande du Procureur Général, du juge d'instruction ou des officiers de police judiciaire agissant sur réquisition du Procureur Général ou du juge d'instruction dans le cadre d'une investigation en cours ».

C'est en application de ces dispositions que la Commission demande très fréquemment aux entités assujetties de se conformer à ces délais légaux, et de ne proroger le délai de 5 ans que dans les cas limitatifs légalement prévus, et justifiés au cas par cas.

Les demandes de la Commission concernent également les délais de conservation des demandes d'information émanant selon les cas de l'AMSF, du Conseil de l'Ordre des Avocats, du Procureur Général ou du Juge d'instruction, pour lesquelles l'article 24 de la Loi n° 1.362 fixe la durée maximale de conservation à un an.

De ce fait la CCIN limite à cette durée de conservation la demande d'information elle-même, mais également les informations relatives à la personne ayant fait l'objet de cette demande, que la personne soit connue de l'entité assujettie ou non, et ce afin de ne pas permettre la constitution d'une liste d'exclusion. En ce sens la Commission relève également qu'une procédure existe en vertu de l'article 53 de la Loi n° 1.362, modifiée, qui dispose que « *Le service exerçant la fonction de renseignement financier de l'Autorité peut, pour une durée maximale de six mois, renouvelable, désigner aux organismes et personnes mentionnés aux articles premier et 2, pour la mise en œuvre de leurs obligations de vigilance (...). 2°) des personnes qui présentent un risque important de blanchiment de capitaux, ou de financement du terrorisme et de la prolifération des armes de destruction massive* ». Aussi la CCIN considère que les demandes de renseignements / d'information de l'AMSF ne peuvent se substituer à ce mécanisme existant.

Si les durées de conservations susmentionnées sont légalement encadrées, tel n'est pas le cas des informations relatives aux déclarations de soupçons effectuées par les entités assujetties. Il incombe alors à la CCIN de les fixer, en tenant compte notamment de la nature desdites informations et de l'article 10.1 de la Loi n° 1.165 qui dispose que les informations nominatives doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées ou pour laquelle elles seront traitées ultérieurement* ».

Aussi, s'il arrive que les responsables de traitements souhaitent conserver les déclarations de soupçon 10 ans après la déclaration si celle-ci est demeurée sans suite, la CCIN fixe les durées de conservation comme suit :

- 5 ans après la déclaration demeurée sans suite de la part de l'AMSF ;
- 6 mois après l'information par l'AMSF de l'existence d'une décision judiciaire devenue définitive ;
- 1 an maximum à compter de l'alerte si celle-ci ne donne lieu à aucune déclaration.

Les principes rappelés ci-dessus s'appliquent également aux traitements non automatisés, dès lors que les informations nominatives sont contenues dans un ensemble structuré, et qu'elles sont accessibles selon des critères déterminés : article 24-1 de la Loi n° 1.165.

Les autorisations de transfert vers un Pays ne disposant pas d'un niveau de protection adéquat

En 2023, la Commission a délivré 24 autorisations de transferts d'informations nominatives.

Dans le cadre de l'instruction de ces dossiers elle a identifié plusieurs points qui posaient des difficultés aux responsables de traitement et a porté une attention toute particulière sur les éléments suivants.

Le choix de la finalité

Le principe : le responsable de traitement doit effectuer une formalité par finalité de transfert (ex. maintenance, analyse des alertes, support client, etc.). Conformément à l'article 10-1 la finalité doit être « *déterminée et explicite* ». Ainsi, il convient normalement d'indiquer, outre l'objectif poursuivi par le transfert, le pays et l'entité destinataire (ex. prestataire, société du groupe, etc.), s'il s'agit d'un envoi de données vers un pays hors protection adéquate, ou simplement d'un accès depuis un de ces pays, au système d'information du responsable de traitement situé à Monaco.

Exemple d'une finalité telle que modifiée par la Commission : « *Réception des alertes « Data Loss Prevention » par l'équipe en charge de l'analyse de ces alertes sise à Singapour dans le cadre des échanges avec les salariés de Monaco* ».

La Commission met à disposition des responsables de traitement, sur son site Internet la liste des pays disposant d'un niveau de protection adéquat.

La justification du transfert

En application de l'article 20-1 de la Loi n° 1.165 un transfert d'informations nominatives vers un pays ne bénéficiant pas d'un niveau de protection adéquat peut être effectué sous certaines conditions.

Le premier alinéa de cet article dispose que le transfert peut avoir lieu notamment si :

- la personne concernée a donné son consentement ;

La Commission rappelle que les personnes concernées peuvent retirer leur consentement à tout moment.

Ainsi, lorsque le consentement est utilisé comme fondement pour le transfert et que la personne concernée le retire, le responsable de traitement doit stopper immédiatement tout transfert d'informations.

Le consentement doit aussi être libre et éclairé. Ainsi, impossible de consentir à un captcha[5] procédant à un transfert (ex. le reCAPTCHA de Google), car la personne concernée n'accède pas au service si elle refuse. Le consentement n'est donc pas libre.

- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat ;

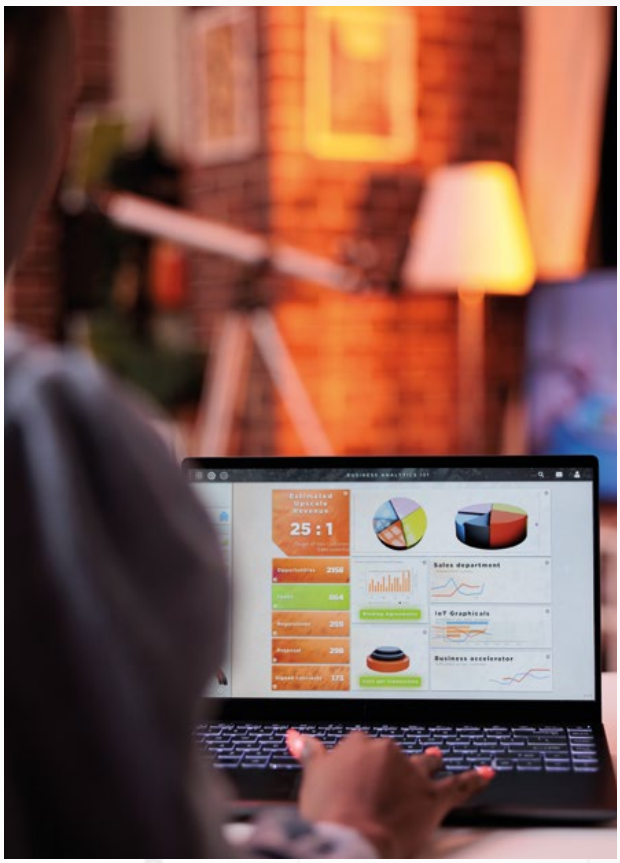
- le transfert est nécessaire à la sauvegarde de l'intérêt public.

La Commission estime que les transferts effectués sur ces deux fondements ne peuvent être systématiques et doivent se limiter au transfert « *nécessaire* » à la conclusion ou à l'exécution du contrat ainsi qu'à la sauvegarde de l'intérêt public. De plus, le transfert des informations nominatives concernées doit être proportionné.

Ainsi, la Commission demande systématiquement aux responsables de traitement d'évaluer les critères de nécessité et de proportionnalité avant tout transfert d'informations.

C'est sur ces deux fondements qu'une autorisation de transfert a été délivrée en vue de la communication potentielle d'informations vers la Securities Exchange Commission des Etats-Unis d'Amérique (délibération n° 2023-160).

[5] Test de Turing public complétement automatisé permettant de différencier un utilisateur humain d'un ordinateur



Par ailleurs, conformément à l'alinéa 2 de l'article précité, le transfert d'informations nominatives peut également avoir lieu « *lorsque le responsable de traitement, ou son représentant, ainsi que le destinataire des informations offrent des garanties suffisantes* ». Au cours de l'instruction des demandes d'autorisation de transfert qui lui ont été soumises, la Commission a constaté que deux types de garanties sont le plus souvent utilisées par les responsables de traitement :

- les clauses contractuelles

La Commission considère que des clauses contractuelles peuvent constituer des garanties suffisantes dans le cadre d'un transfert si celles-ci prévoient notamment :

o les droits et obligations des parties ;

o le respect des principes applicables au traitement des données personnelles ;

o la mise en œuvre de mesures de sécurité ;

o la question des éventuels transferts ultérieurs de données ;

o les droits des personnes concernées.

Enfin, la Commission considère que le recours aux clauses contractuelles types (CCT) approuvées par l'Union européenne est possible à condition que ces dernières soient complétées en prenant en compte les spécificités monégasques et notamment que les droits des personnes concernées à Monaco soient effectifs, et que la CCIN puisse s'assurer de l'application des CCT, au même titre que les Autorités de contrôle de l'Union européenne, quand des données en provenance de Monaco sont concernées.

- les règles d'entreprise contraignantes

Les règles d'entreprise contraignantes sont utilisées pour encadrer les transferts d'informations nominatives au sein d'un groupe de sociétés.

Afin d'autoriser un transfert sur ce fondement la Commission prend en considération, lors de l'instruction du dossier, divers éléments dont notamment :

o le(s) transfert(s) ou catégories de transferts concernés, la(es) finalité(s) poursuivie(s) par le transfert ainsi que la finalité du traitement à l'origine du transfert, les données personnelles ou les catégories de données personnelles transférées, ainsi que les personnes concernées ;

o le respect des principes relatifs à la qualité des informations nominatives et aux conditions de licéité ;

o le respect des droits et libertés des personnes concernées ;

o les mesures de confidentialité et de sécurité mises en œuvre ;

o le respect des dispositions de la Loi n° 1.165.

L'information des personnes concernées

La Commission constate de manière récurrente que les mentions d'information jointes aux dossiers ne sont pas conformes aux exigences légales. Ainsi, elle rappelle souvent dans ses délibérations que ces mentions doivent contenir, en plus des éléments prévus à l'article 14 de la Loi n° 1.165, des informations telles que :

- la finalité du traitement à l'origine du transfert ;
- la finalité du transfert lui-même ; et
- l'usage qui sera fait des données personnelles par les destinataires ou catégories de destinataires.

Par ailleurs, des informations complémentaires peuvent être requises en fonction du traitement (ex. informations spécifiques à insérer dans le bandeau cookies lorsque le module Google Analytics est utilisé).

La sécurité du transfert

Le responsable de traitement doit également fournir à la Commission des informations relatives à la sécurité du transfert notamment des éléments portant sur :

- la sécurité du transfert d'information (ex. comment sont communiquées les informations ? (de serveur à serveur, par le biais d'un service cloud, par le biais d'une messagerie électronique, etc.), comment les informations sont-elles protégées ? (système d'habilitation, chiffrement, pseudonymisation, etc.)) ; ou
- la procédure selon laquelle un accès est accordé depuis un pays ne disposant pas d'un niveau de protection adéquat (ex. qui a accès ?, comment ?, pourquoi ?, etc).

Par ailleurs, le responsable de traitement doit communiquer des informations relatives à la sécurité du système dit de « *destination* » et/ou des personnes disposant d'un accès distant à ses serveurs d'information.

Enfin, la demande d'autorisation de transfert doit être accompagnée de schémas techniques illustrant les flux de données ainsi que les mesures de sécurité mises en place (VPN, HTTPS, pares-feux, antivirus, etc.).

Au cours de l'année 2023 la Commission a été saisie, à plusieurs reprises, de questions relatives aux choix des prestataires de Cloud lorsqu'il s'agit d'entreprises dont le siège est situé dans des pays hors protection adéquate.

A cet égard, il convient de rappeler que ce choix doit être guidé par une analyse effectuée par le responsable de traitement. Ainsi, si certains prestataires ont leur siège dans un pays non adéquat, ils peuvent mettre à disposition des services Cloud hébergés et sauvegardés exclusivement en Europe.

Toutefois, en fonction des prestataires et des offres, des salariés du prestataire localisés dans un pays hors protection adéquate, peuvent être susceptibles d'avoir accès aux informations du responsable de traitement.

A cet égard, certains prestataires ont mis en place des mesures permettant à leurs salariés d'avoir accès aux informations de leurs clients en toute sécurité par le biais de procédures permettant au responsable de traitement d'autoriser l'accès et d'assurer le suivi et la traçabilité des actions du prestataire. Pour d'autres, aucune demande d'autorisation de transfert des données ne sera nécessaire car l'accès à la donnée est tout simplement impossible by design.

Si le responsable de traitement constate qu'il y a un transfert de données, il doit assurer la sécurité des informations qu'il dépose sur le cloud en fonction de leur sensibilité. Il pourra par exemple procéder au chiffrement de ses données avec une clé qui n'est pas celle fournie par le prestataire en question.

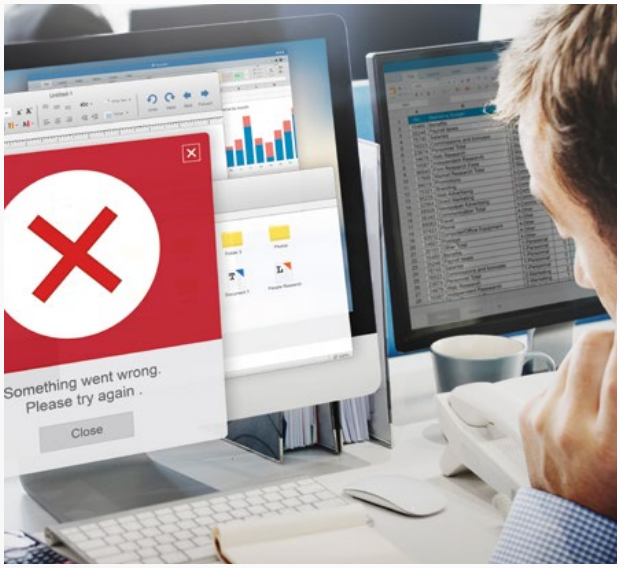
Enfin, la CCIN constate l'utilisation de prestataires gratuits « *tout en un* » pour la constitution de sites Internet qui ne répondent pas toujours aux exigences de la Loi n° 1.165, et avec lesquels le responsable de traitement ne peut pas facilement moduler ses exigences pour être en conformité avec la Loi.

→ Lorsqu'elle n'est pas en mesure d'obtenir les informations souhaitées, la Commission refuse l'autorisation de transfert qui lui est soumise. Ceci a été le cas pour une demande de transfert examinée en 2023 et pour laquelle les destinataires précis des informations n'étaient pas identifiés de même que leurs missions exactes, le responsable de traitement mentionnant les équipes responsables de la gestion des données, de l'informatique, de l'analyse statistique, ... ainsi que plusieurs fournisseurs, sans toutefois préciser l'ensemble de ces entités ni leurs rôles.

Aussi la commission n'a pas été en mesure d'appréhender l'étendue du transfert (destinataires, catégories de données transférées) ni la finalité du transfert selon les différents destinataires.

Enfin, le transfert étant justifié par le consentement des personnes concernées, elle a relevé que l'information préalable qui leur était délivrée ne leur permettait pas de consentir à ce transfert de manière éclairée.

En conséquence le responsable de traitement n'a pas été autorisé à procéder au transfert d'informations.



LES REFUS D'AUTORISATION ET LES AVIS DÉFAVORABLES DE LA COMMISSION

Si la Commission a rendu, en 2023, 163 avis favorables et autorisations, elle s'est prononcée à 5 reprises défavorablement à la mise en œuvre de traitements automatisés d'informations nominatives pour les diverses raisons suivantes.

L'encadrement strict de l'utilisation de dispositifs biométriques

Lors de sa réunion du 18 octobre 2023, la Commission a émis deux refus à la mise en œuvre de dispositifs biométriques et a profité de l'occasion pour rappeler aux responsables de traitement qu'elle encadrait strictement l'utilisation de ces dispositifs dès lors qu'ils reposaient sur la reconnaissance de l'empreinte digitale ou la reconnaissance faciale.

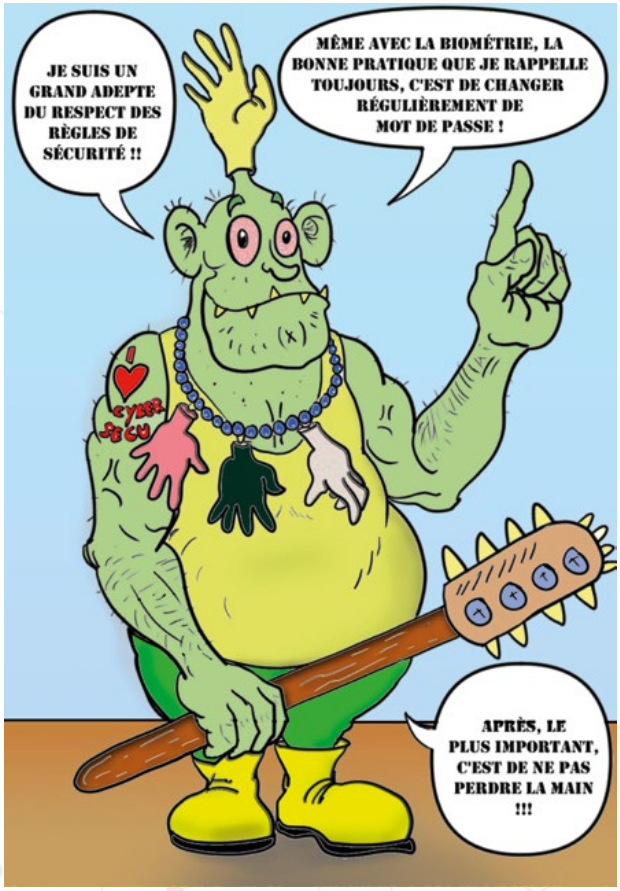
La Commission considère en effet que les méthodes de reconnaissance de l'empreinte digitale et de reconnaissance faciale posent des difficultés spécifiques en ce que les données ainsi collectées constituent une biométrie particulièrement traçante.

Ces données ne sont en effet pas attribuées par un tiers ou choisies par la personne mais proviennent directement du corps de la personne concernée et la désignent de façon définitive. En conséquence, le mauvais usage ou le détournement de telles données peut avoir des conséquences graves.

Le premier dispositif était un contrôle d'accès biométrique reposant sur la reconnaissance de l'empreinte digitale stockée sur un boitier centralisé.

Or, conformément à sa délibération n° 2011-33 du 11 avril 2011, la Commission a indiqué qu'elle n'autorisait le recours aux dispositifs portant sur la reconnaissance de l'empreinte digitale, que lorsque le stockage de la donnée biométrique se fait sur un support individuel, détenu uniquement par la personne concernée.

Pour plus d'informations, voir la Délibération n° 2011-33 du 11 avril 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale, exclusivement enregistrée sur un support individuel détenu par la personne concernée, ayant pour finalité le contrôle d'accès à des zones limitativement identifiées sur le lieu de travail, mis en œuvre par les personnes physiques ou morales de droit privé.



Le second dispositif était un logiciel de reconnaissance faciale que le responsable de traitement voulait interfacer avec le système de vidéosurveillance précédemment autorisé par la Commission.

Les justifications avancées par le responsable de traitement étaient :

- le consentement des personnes concernées, en ce que le dispositif de reconnaissance faciale visait à détecter les personnes dont les données biométriques n'avaient pas été préalablement enrôlées. Aussi ledit dispositif concernait essentiellement les salariés.

La Commission n'a pas accepté cette justification en rappelant que compte tenu du lien de subordination liant l'employeur à ses salariés, le consentement de ces derniers ne pouvait être donné librement ;

- la réalisation d'un intérêt légitime qui consistait en l'espèce à assurer la sécurité des locaux en prévenant l'opérateur de vidéosurveillance de tout accès aux locaux par des personnes qui n'auraient pas préalablement été enrôlées dans le dispositif de reconnaissance faciale. Là encore la Commission a rejeté cette justification en soulignant que le responsable de traitement ne démontrait pas la nécessité de recourir à un tel dispositif, très encadré par la CCIN. Ainsi, d'autres moyens moins intrusifs pour les personnes concernées pouvaient être mis en place afin d'atteindre le même objectif de sécurisation de l'accès aux locaux (contrôle d'accès par badge par exemple).

Extrait de la délibération de la CCIN portant refus à l'utilisation d'un dispositif de reconnaissance faciale :

« La Commission rappelle que la donnée biométrique n'est pas une donnée d'identité comme les autres. Elle n'est pas attribuée par un tiers ou choisie par la personne. Elle provient de son corps lui-même et

le désigne de façon définitive. Le mauvais usage ou le détournement d'une telle donnée peut alors avoir des conséquences graves.

La Commission encadre donc strictement cette méthode.

Aussi, après avoir relevé que le dispositif est mis en place uniquement dans un but sécuritaire, afin d'assurer la sécurité des biens et des personnes, elle considère qu'il appartient au responsable de traitement de démontrer la nécessité de recourir à un tel dispositif de reconnaissance faciale en indiquant les raisons pour lesquelles le recours à d'autres mesures organisationnelles et techniques ou bien encore à d'autres dispositifs d'identification, tels que par exemple des badges, ne permet pas d'atteindre le niveau de sécurité exigé.

La Commission estime en conséquence que cette justification doit impérativement détailler le contexte spécifique rendant nécessaire un niveau de protection élevé ainsi que les raisons justifiant l'utilisation de la biométrie plutôt qu'une autre technologie, ce qui n'est pas le cas en l'espèce.

Elle relève enfin qu'outre l'identification biométrique, les nom et prénom des personnes concernées seront désormais également collectées.

Or, la Commission rappelle que les informations collectées doivent être « adéquates, pertinentes et non excessives » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

A cet effet, elle considère que la collecte de l'identification biométrique ainsi que des nom et prénom dans le cas de l'exploitation de ce traitement apparaît manifestement excessive au regard des fonctionnalités dudit traitement. En effet, cette collecte en vue d'assurer la sécurité des biens et des personnes peut conduire à une surveillance pouvant être inopportune à l'égard des personnes concernées.

En conséquence, en l'absence de justification démontrant la nécessité d'installer un dispositif de reconnaissance faciale interfacé avec le système de vidéosurveillance pour contrôler les accès aux locaux de la société, la Commission exclut expressément l'utilisation de ce dispositif à des fins de sécurité des biens et des personnes au sein desdits locaux. »

La non-conformité d'un prestataire

Le traitement soumis à la Commission concernait la gestion des opérations éditiques d'un responsable de traitement du secteur public, qui souhaitait confier à un prestataire les impressions des documents émis par ses différents Services, et leur expédition. Compte tenu de la nature de certains de ces documents, la Commission a relevé que, si une clause de confidentialité liait bien le prestataire dans le cadre de son contrat de sous-traitance, ledit prestataire n'avait effectué aucune formalité auprès de la CCIN, la privant ainsi de toute possibilité de s'assurer de la sécurité des informations traitées pour le compte du responsable de traitement.

Peu après cet avis défavorable émis par la Commission, le prestataire lui a soumis le traitement relatif à la plateforme de dépôt des documents, faisant apparaître les mesures de sécurité y associées. Aussi un avis favorable a en définitive pu être émis par la CCIN afin de permettre au responsable de traitement de déléguer les impressions de documents.

L'impossibilité d'apprécier la proportionnalité des dispositifs envisagés en matière de traçabilité des flux sortants

En 2023 la Commission a refusé la mise en œuvre à deux reprises de traitements liés à la traçabilité des flux sortants. Si ces dispositifs sont de plus en plus déployés aux fins d'éviter la fuite de données confidentielles, il n'en demeure pas moins que la CCIN veille à la précision du périmètre exact de ces outils qui peuvent être déployés sur différents canaux de communication (flux Internet, messagerie professionnelle et / ou instantanée, ..)[6] , ainsi qu'à la qualité de l'information délivrée aux salariés qui doit se faire outil par outil afin qu'ils puissent adapter leur comportement, mais également à la proportionnalité dans l'utilisation de ces dispositifs qui peuvent être particulièrement intrusifs pour les personnes qui y sont soumises.

Dans le cadre de l'examen de deux de ces dossiers, la Commission a constaté qu'en dépit des demandes de précisions formulées aux responsables de traitement concernés, aucune information complémentaire ne lui était parvenue.

Ainsi notamment elle n'a pu obtenir aucune information sur la nature et l'utilisation qui serait faite d'un rapport mensuel qu'il était envisagé d'établir concernant l'ensemble des emails des collaborateurs.

Constatant que les informations dont elle disposait étaient bien trop lacunaires afin d'être en capacité de s'assurer du périmètre exact du contrôle mis en place à l'égard des salariés, et donc de sa proportionnalité, ainsi que des mesures de sécurité afférentes aux traitements qui lui étaient soumis, la Commission a refusé leur mise en œuvre.

[6] Sur les outils de prévention des fuites de données voir Rapport d'activité CCIN 2022 p 54 et suivantes

4

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.

Elle participe fréquemment à des manifestations dédiées à la protection des données afin d'échanger avec ses homologues, ainsi qu'avec des spécialistes de la matière.

Réunion de travail sur la protection des données personnelles dans l'aide humanitaire internationale

Le 21 mars 2023, la CCIN a accueilli dans ses locaux une réunion du groupe de travail sur le rôle de la protection des données personnelles et

de la vie privée dans l'aide internationale au développement, l'aide humanitaire internationale et la gestion de crise (« *GTAID* ») dont elle assure la vice-présidence.

L'objectif de cette réunion était d'analyser les réponses au questionnaire que le groupe avait envoyé aux principaux acteurs de l'aide internationale afin de comprendre leurs pratiques en matière de protection des données personnelles et d'identifier les problématiques urgentes.

Etaient présents le Préposé fédéral à la protection des données et à la transparence (PFPDT) - Suisse, Président du Groupe, l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP), l'Autorité de Protection des Données à caractère Personnel du Bénin (APDP), la Commission Nationale pour la Protection des Données du Luxembourg (CNPD) et le Haut-Commissariat des Nations Unies pour les Réfugiés (UNHCR).

Présence de la CCIN au Forum INCYBER autour du thème « *In Cloud we trust ?* »

À l'occasion de la 15ème édition du Forum INCYBER (anciennement FIC), des agents de la CCIN se sont rendus à Lille au Grand Palais pour assister aux séances plénières, conférences, démonstrations tech-niques, démonstrations d'attaque, FIC Talk et Masterclass de cet événement de cybersécurité et de confiance numérique.

En sus des thèmes récurrents de la sécurité numérique tels que l'identité numérique, la lutte anti-cybercriminalité, le management des cyber-risques et le KYC (Know Your Customer), le public présent a constaté durant cette édition un élargissement des thématiques et propositions ; la CCIN a ainsi pu assister à des démonstrations d'attaques en matière de cybersécurité industrielle ou encore participer à des échanges autour de l'OSINT ou « *Open Source Intelligence* » (renseignement de Source Ouverte en français), un élément fondamental pour les opérations de renseignements.

Par ailleurs Vincent Strubel, Directeur de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) a tenu à souligner lors de sa prise de parole que « *Tous les cloud ne se valent pas* », tout en reconnaissant que « *nous ne sommes pas d'accord avec beaucoup de monde sur le sujet du cloud* » pour conclure sur l'observation que « *nous avons tous besoin de lutter contre cette idée que le cloud est une solution sécurisée* ».

Pour le directeur de l'ANSSI, le recours au cloud doit être « *réfléchi* » et enjoint les responsables de traitements à « *bien lire les petites lignes des contrats* ».
D'autres temps forts ont marqué cette 15ème édition du FIC, comme l'intervention du Commissaire européen au marché intérieur, Monsieur Thierry Breton, qui s'est exprimé à propos du rôle de l'Europe en matière de cyber-résilience en soulignant que « *si l'Europe est devenue un acteur politique, économique et sécuritaire mondial, elle est aussi une cible*

de plus en plus importante pour les cyberattaques » en annonçant qu'un milliard d'euros sera notamment alloué à la construction de plusieurs SOC « *Systems and Organizations Control* » (cadre utilisé pour aider les entreprises à démontrer les contrôles de sécurité qui sont en place pour protéger les données des clients dans le cloud) afin de créer un « bouclier cybersécurité » pour identifier le plus en amont possible les attaques informatiques en Europe.

Participation à la conférence de Printemps de l'IAPP à Washington D.C.

La Conférence annuelle de l'International Association of Privacy Professionals (IAPP) sur la protection de la vie privée s'est tenue du 2 au 5 avril 2023 à Washington, D.C. en présence d'un agent du Secrétariat de la CCIN.

Après une première journée dédiée aux Autorités de protection des données pendant laquelle ont été évoquées notamment la Loi sur la protection des données personnelles du consommateur en Californie (CCPA) et la mise en place d'une nouvelle Cour d'examen de la protection des données personnelles dépendant du ministère de la Justice américain, les jours suivants ont été consacrés aux derniers développements en matière de vie privée dans le monde.

Deux sujets ont été au centre de toutes les attentions. Le développement de l'intelligence artificielle générative a ainsi fait l'objet de plusieurs tables rondes. Lors de la session d'ouverture, la conférencière Nina Schick, a par ailleurs insisté sur le fait que s'il a fallu 10 mois à Facebook pour atteindre 1 million d'utilisateurs en 2004, ChatGPT a réalisé cet exploit en seulement cinq jours en 2022, soulignant en conséquence la nécessité pour les Gouvernements et les organismes de règlementation de développer des mécanismes de contrôle à un rythme beaucoup plus rapide.

L'autre point d'attention est l'incertitude pesant encore sur les échanges transfrontaliers entre l'Union européenne et les Etats-Unis suite à l'invalidation du Privacy Shield par la Cour de justice de l'Union

européenne le 16 juillet 2020. Si le président américain, Joe Biden, et la présidente de la Commission européenne, Ursula Von Der Leyen, ont annoncé qu'ils s'étaient mis d'accord sur le principe d'un nouveau cadre de protection des données entre l'Union européenne et les Etats-Unis, celui-ci ne présente pas encore toutes les garanties suffisantes, notamment en matière de droits des personnes concernées, de transferts ultérieurs ou encore d'accès aux données par les agences de renseignements américaines. Présent lors de la session de clôture, l'activiste Max Scrhrems, à l'origine de l'invalidation des deux premiers instruments de transfert, a d'ores et déjà indiqué qu'il contesterait cet accord si la Commission européenne devait l'adopter.

Table ronde organisée par l'ECRI à Monaco en coopération avec le Haut-Commissariat à la protection des Droits, des Libertés et à la Médiation

A l'invitation du Haut-Commissariat, la CCIN a été invitée à prendre part à la table ronde organisée le 25 avril 2023 par la Commission européenne contre le racisme et l'intolérance (ECRI) sur la prévention et la lutte contre le racisme et l'intolérance. Cet événement fait suite à la publication du rapport de l'ECRI sur Monaco en juin 2022. L'objectif a été d'avoir des échanges sur les suites données ou à donner aux recommandations contenues dans ce rapport. La table ronde a été divisée en trois sessions à savoir, les principales constatations de l'ECRI (politiques d'inclusion), l'organisme de promotion de l'égalité, la lutte contre le discours de haine.

Outre les représentants des Autorités nationales et locales, la table ronde a réuni des membres d'organisations de la société civile, ainsi que des membres des groupes relevant du mandat de l'ECRI. Cet évènement a permis de contribuer positivement au débat national sur la lutte contre la discrimination et l'intolérance dans le pays.

Dans son rapport de 2022 sur Monaco, l'ECRI s'est déclarée préoccupée par des questions telles que la nécessité d'adopter une législation régissant la lutte contre

De droite à gauche : Johan FRIESTEDT, Secrétaire Exécutif de l'ECRI ; Kristina PARDALOS, membre de l'ECRI ; Bertil COTTIER, Vice-Président de l'ECRI; Patrice DAVOST, membre de l'ECRI au titre de Monaco ; Marina CEYSSAC, Haut-Commissaire à la Protection des Droits ; Isabelle ROSABRUNETTO, Directeur Général du Département des Relations Extérieures et de la Coopération ; Corinne BOURDAS MAGAIL, Chargé de Mission auprès du Département des Relations Extérieures et de la Coopération. Copyright : Studio Phénix

toutes les formes de discrimination et de renforcer les pouvoirs du Haut-Commissaire, notamment en matière d'enquêtes, la nécessité de permettre aux Autorités judiciaires de lutter plus efficacement contre les discours de haine en ligne, la nécessité de supprimer toute différence de traitement injustifiée entre les couples de même sexe et les couples de sexe opposé, la nécessité d'inclure dans le droit interne une procédure de traitement des demandes d'asile conformément au droit international et d'établir des normes claires régissant le droit au regroupement familial et aux permis de séjour, la nécessité de ratifier la Charte sociale européenne révisée, d'interdire des licenciements sans motif préalable et valable et de prendre des mesures efficaces pour garantir l'accès au logement des résidents étrangers.

Cette participation a été l'occasion pour la CCIN de rappeler son intervention fréquente pour obtenir la suppression rapide de contenus publiés en ligne, et sur les réseaux sociaux, portant atteinte aux personnes concernées.

La Conférence annuelle de l'AFAPDP

C'est à 14 kilomètres à peine de l'Europe, à Tanger, au Maroc, que s'est tenue le 2 octobre la 14ème conférence des Autorités Francophones de Protection des Données Personnelles (AFAPDP), à laquelle 2 agents du Secrétariat ont participé.

Cette année le thème central de la journée était le « *data scraping* » ou moissonnage des données en français qui consiste en l'extraction automatisée d'informations personnelles à partir d'Internet. Cette pratique comporte en effet un certain nombre de risques pour les données, dont notamment les cyberattaques ciblées, l'usurpation d'identité, le profilage, les spams ou encore la prospection directe non autorisée.

Le Commissariat à la protection de la vie privée du Canada (CPVP/OPC), la Commission nationale pour le contrôle des données à caractère personnel (CNPD) du Maroc et le Préposé fédéral à la protection des données et à la transparence (Suisse) ont ainsi présenté la prise de position commune qu'ils ont publiée avec 9 autres Autorités de protection, qui recommande aux entreprises du numérique de prendre un certain nombre de mesures.

Parmi celles-ci figurent la désignation de responsables de la protection contre le scraping, la limitation du nombre de pages consultées par heure par le même utilisateur ou encore l'identification du trafic de « *bots* » (robots).

Les autorités recommandent par ailleurs aux utilisateurs qui souhaitent se protéger de lire les informations mises à disposition par les plateformes concernant la transmission des données, ainsi que de comprendre et de gérer les paramètres de confidentialité.

La Commission nationale de l'informatique et des libertés (CNIL) de son côté a présenté son projet de guide pratique sur l'ouverture et la réutilisation des données publiquement accessibles.

L'après-midi, un tour de table des évolutions et actualités législatives en matière de protection des données personnelles dans l'espace francophone a été organisé ; l'occasion pour la CCIN de présenter le projet de Loi, actuellement en cours d'examen, ayant pour objet la refonte du droit des données personnelles monégasque.

Enfin, le lendemain, lors de sa 14ème Assemble Générale, l'association a accueilli en son sein les Autorités de Georgie, du Kosovo et de la Mauritanie, portant le nombre de ses membres à 26.

La CCIN invitée à partager avec les acteurs du numériques lors de la 23ème édition des Assises de la sécurité

Du 11 au 13 octobre se sont tenues en Principauté, les Assises de la sécurité dont le thème était pour cette 23ème édition, « *Prenons de la hauteur* » car si, comme l'ont souligné les intervenants, les avancées sont nombreuses dans le domaine de la cybersécurité, il est plus que jamais nécessaire pour les acteurs du numérique de partager leurs expériences afin de préparer les crises de demain.

L'évènement s'est ainsi ouvert par une allocution du Ministre d'Etat, Monsieur Pierre Dartout, qui a rappelé que Monaco avait « *décidé d'aligner son cadre réglementaire en matière de sécurité numérique sur celui de la Directive européenne afin de garantir que les échanges entre la Principauté et l'UE, qui reste le partenaire privilégié de la Principauté, se fassent dans les mêmes conditions de sécurité que dans le marché intérieur de l'Union européenne* ».

Monsieur Philippe Lecouffen, Directeur des opérations d'Europol, a lui aussi souligné l'importance d'une coopération internationale en appelant les experts présents à échanger des informations en temps réel sur les menaces toujours plus nombreuses dans un contexte qui évolue de plus en plus rapidement.

Enfin, Monsieur Vincent Strubel, a mis en avant les trois défis auxquels l'Agence nationale de la sécurité de systèmes d'information (ANSSI), dont il est le nouveau Directeur général, était confrontée : « *tirer vers le haut et faire gagner en maturité les petits, se préparer à la crise majeure et garder son expertise dans le temps* ».

Pas moins de 3000 personnes ont participé à ce forum qui par le biais d'interventions, de tables-rondes et d'ateliers a réuni des experts du monde entier pour discuter de la géopolitique de la cybersécurité, de la désinformation, des nouvelles menaces et préoccupations des Responsables de la sécurité des systèmes d'information (RSSI) ou encore de l'intelligence artificielle.

L'« *European Case Handling Workshop* », Berne, Suisse

La CCIN a assisté par l'intermédiaire de deux de ses agents à l' « *European Case Handling Workshop* » (ECHW) qui s'est tenu à Berne les 8 et 9 novembre 2023.

Cet événement a réuni 80 représentants de 37 Autorités de protection des données personnelles, provenant

de 27 Etats, dans l'objectif d'échanger sur des questions pratiques auxquelles sont confrontées les Autorités dans l'exercice de leurs missions.

L'événement était scindé en 13 ateliers animés par des membres de différentes Autorités. Ils étaient organisés sous la forme de courtes présentations qui donnaient ensuite lieu à des discussions ouvertes par rapport à des scénarios rencontrés dans l'exercice de leurs activités.

Certains ateliers étaient dédiés à des questions relatives aux procédures que les Autorités peuvent mettre en place dans l'exercice de leurs missions. Les sujets abordés concernaient notamment le traitement des plaintes transfrontalières, l'approche à adopter dans le cadre de demandes non fondées ou excessives, la coopération entre Autorités ou encore le traitement des violations de données personnelles.

Des ateliers portant sur des sujets plus techniques ont également été organisés avec notamment des discussions autour de la surveillance des salariés par GPS, durant lesquelles le respect des obligations des responsables de traitement (information des salariés, délimitation de la finalité poursuivie, identification de la base légale) a été rappelé.

Aussi, un atelier a porté sur les « *deceptive design patterns* », que l'on peut traduire par interfaces trompeuses en français. Dans le cadre de celui-ci, différents scénarios proposés par des membres du Comité européen de la protection des données (CEPD) ont été analysés à l'aune des Lignes directrices 03/2022 du CEPD relatives aux interfaces trompeuses sur les réseaux sociaux.

Enfin, un dernier atelier organisé par l'Autorité italienne avait pour objet la distinction entre reconnaissance faciale et détection faciale. Plus particulièrement, les discussions ont tourné autour d'une sanction rendue par ladite Autorité le 13 avril 2023 à l'encontre de la ville de Bologne sur un système de détection faciale mis en place dans un musée qui souhaitait comprendre la manière d'interagir des visiteurs avec les œuvres d'art exposées. L'Autorité italienne a conclu que la mise en œuvre d'un dispositif de détection faciale, même sans conservation des images des visiteurs était soumise, tout comme la mise en œuvre d'un dispositif de reconnaissance faciale, au respect des règles relatives à la protection des données personnelles.

La CCIN s'associe à la Journée internationale pour l'élimination de la violence à l'égard des femmes

Le 25 novembre est la Journée internationale pour l'élimination de la violence à l'égard des femmes. A cette occasion le Comité monégasque pour la promotion et la protection des droits des femmes a invité la CCIN à prendre part aux manifestations organisées en Principauté.

Placée cette année sous le thème des violences numériques, la célébration de cette journée a pour objet de sensibiliser notamment le jeune public aux dangers de l'utilisation des réseaux sociaux.

En complément du manga réalisé par le Comité monégasque, la CCIN a édité son propre flyer sur les bons réflexes à adopter, et les pratiques à éviter.

Pour plus d'informations sur cette journée et les activités du Comité :

https://dfm.mc/communique_de_presse/un-manga-pour-parler-des-violences-numeriques-pour-le-25-novembre-2023/

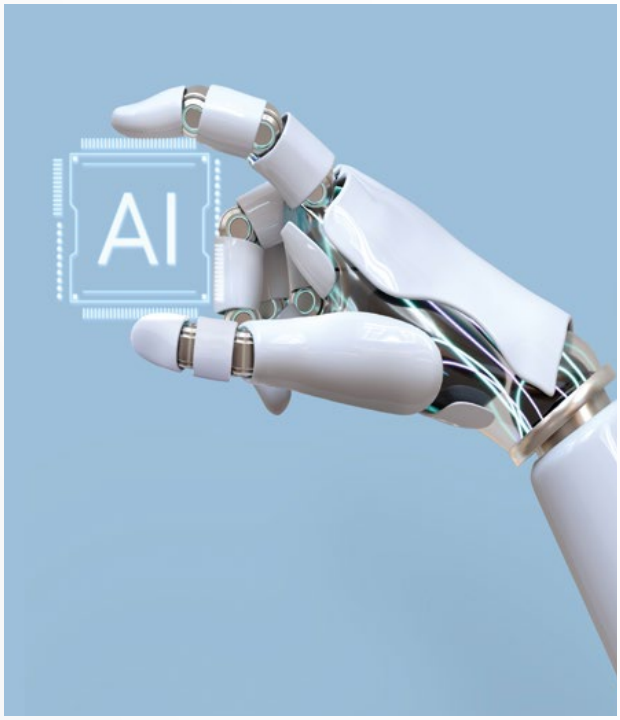
Déplacement à Ottawa pour la 72ème rencontre du Groupe de Berlin et le Symposium international sur la protection de la vie privée et l'IA générative

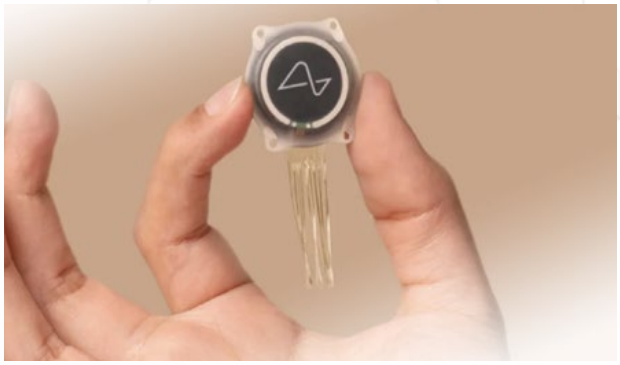
Début décembre, un agent du Secrétariat s'est rendu à Ottawa, Canada, pour assister à la réunion du Groupe de travail international sur la protection des données dans les technologies, dît « *Groupe de Berlin* », coprésidé pour l'occasion par le Commissariat à la protection de la vie privée du Canada (CPVP OPC) et le Commissaire fédéral à la protection des données et à la liberté d'information de l'Allemagne.

Au programme, des sujets d'actualité allant du partage des données personnelles aux nouvelles neurotechnologies ainsi que des discussions fructueuses qui ont abouti à l'adoption d'une résolution sur la Banque Centrale et les monnaies numériques.

Fondé en 1983, le Groupe de Berlin sur la protection des données dans les télécommunications est un groupe de travail international composé de représentants d'Autorités de contrôle nationales de la protection des données, mais aussi de représentants de gouvernements et d'organisations internationales ayant pour mission d'élaborer des propositions et des recommandations au sujet de la protection des données dans les télécommunications.

Cette réunion a été précédée d'un Symposium international sur la protection de la vie privée et l'IA générative organisé par l'OPC pendant lequel les membres du Groupe de Berlin ont pu discuter avec l'ensemble des Autorités en charge de la protection de la vie privée sur le territoire canadien ainsi que des membres du Gouvernement, de l'industrie et de la société civile autour des occasions et risques que présente l'IA générative mais aussi sur la meilleure façon de collaborer pour tous les secteurs afin de s'y préparer.





« *Alors que les technologies comme l'IA générative occupent une place de plus en plus grande dans nos vies, il sera essentiel de s'assurer que nous sommes en mesure de bénéficier de ces innovations tout en protégeant la vie privée pour réussir en tant que société libre et démocratique, ce qui constituera un défi de taille dans les années à venir* », a déclaré le Commissaire Philippe Dufresne en ouverture du symposium. « *Cette technologie, qui vient changer la donne, exige une approche collective* », a-t-il ajouté.

« *C'est pourquoi nous collaborons étroitement avec nos homologues ici même au pays et à l'étranger pour veiller à ce que l'IA soit conçue et utilisée de manière responsable.* »

5 FICHES THEMATIQUES

LE CLOUD COMPUTING OU LA DONNÉE DANS LES NUAGES

Traduit en français comme « *Informatique dans les nuages* », le Cloud computing ou Cloud est un système de stockage et d'outils qui s'est développé avec la numérisation de la société et qui ne cesse de croître.

Il permet aussi bien de stocker des données personnelles que d'utiliser des logiciels ou même encore de jouer.

En effet, au départ réservé aux professionnels, ce réseau extérieur est désormais utilisé par tout le monde, parfois sans même le savoir ! Ainsi lorsqu'une personne regarde une vidéo, sur une plateforme, le film n'est en général pas téléchargé sur sa tablette, sauf si elle en fait la demande. Elle y accède donc par le cloud du

diffuseur. Il en est de même lorsqu'il y a consultation des e-mails sur smartphone.

La condition d'accès au Cloud est donc d'avoir une connexion internet et un logiciel/une application qui permet l'enregistrement et la consultation des données.

Afin de mieux appréhender ce concept, cette fiche thématique a vocation à présenter le Cloud avec ses principaux avantages et inconvénients, et de mettre en exergue les questions principales qu'il peut poser en matière de protection des données.

Qu'est-ce que le Cloud computing ?

Si les termes de Cloud computing ou de Cloud ne font encore aujourd'hui l'objet d'aucune définition uniformisée, ils recouvrent **l'ensemble des solutions de stockage distant.**

En clair, les données, ou les outils, d'un utilisateur ou d'une entreprise (« *le client* »), ne sont plus sauvegardés sur son disque dur mais sont disponibles sur des serveurs distants accessibles par Internet.

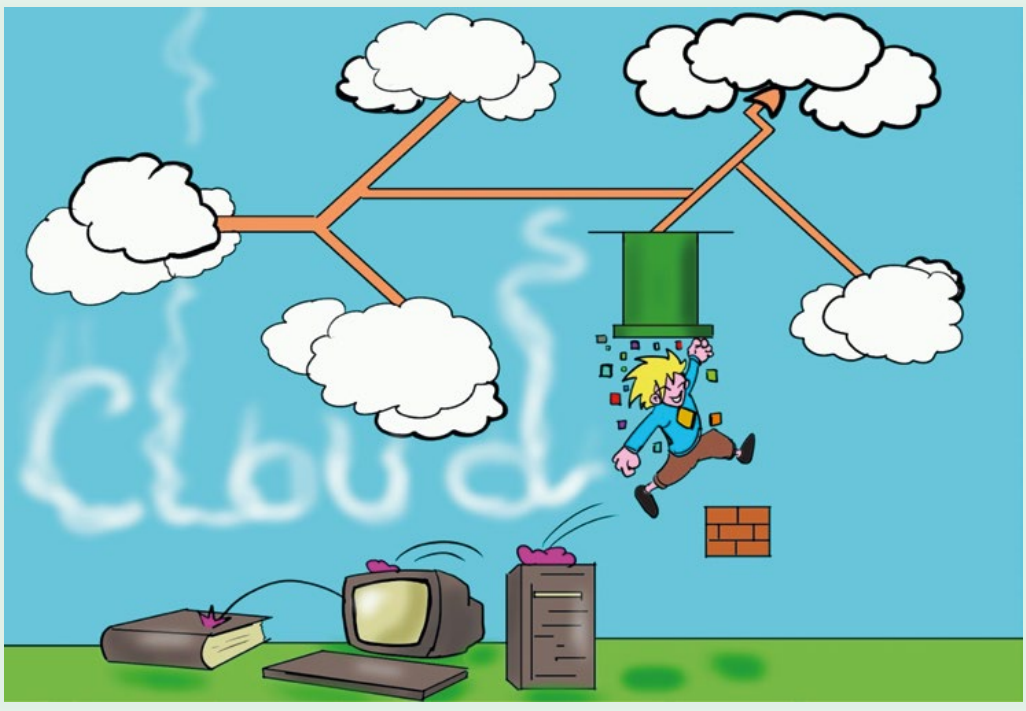
Ces données sont stockées par des infrastructures informatiques loin physiquement de celles du client dans d'immenses salles appelées « *Datacenter* » (centre de données). Ces salles, remplies de serveurs et d'ordinateurs très puissants qui offrent des outils et/ou **enregistrent, stockent, sauvegardent, protègent et administrent** toutes les données envoyées par tous.

Pour le commun des mortels, le Cloud n'est ainsi pas physique mais **virtuel**, et correspond à **un réseau de serveurs distants les uns des autres**, éparpillés sur la planète, mais reliés entre eux et fonctionnant comme un système seul ou bien, maillé.

Il tire son nom du mot anglais signifiant « *nuage* » car au début des années 1990, il était courant de représenter Internet sous forme de nuage dans les schémas de réseaux.

Quant aux données enregistrées dans le Cloud, elles sont, dès connexion à celui-ci, accessibles **n'importe quand, n'importe où et de n'importe quel équipement** connecté à Internet.

Enfin, il est important de noter que certains des systèmes qui utilisent le Cloud comme Google Drive ou iCloud, ont une base gratuite alors que d'autres ne le sont pas (Netflix ou Disney+ par exemple).



Quels sont les différents types de Cloud ?

Il existe quatre principaux types de Cloud.

LE CLOUD PUBLIC

Il s'agit d'un modèle de déploiement de Cloud où les ressources informatiques n'appartiennent pas à l'utilisateur final mais appartiennent à un fournisseur de service Cloud, à savoir une entreprise qui propose des infrastructures, des plateformes et/ou des logiciels via un réseau.

Celui-ci exploite ces ressources informatiques et les partage à l'intention de plusieurs organisations et/ou individus.

Lesdites ressources, accessibles par Internet, sont ainsi **ouvertes à tous et mutualisées.** Les données et applications de chaque client, à savoir toute personne s'exécutant dans le Cloud, restent toutefois isolées et cachées aux autres clients du Cloud.

Le fournisseur est responsable de la maintenance des ressources et garantit la disponibilité, la fiabilité et la sécurité par le biais **d'accords de niveau de service.**

C'est le modèle le plus répandu.

Exemples : AWS (Amazon Web Services), Microsoft Azure

LE CLOUD PRIVÉ

Il s'agit d'un modèle dans lequel l'ensemble des ressources sont réservées via Internet ou sur un réseau interne à **l'usage exclusif d'un groupe d'utilisateurs ou d'une entité clairement défini(e).** Les ressources sont donc inaccessibles à toute personne extérieure.

Les services d'un Cloud privé sont habituellement spécialement conçus pour répondre aux **besoins des clients que ce soit en termes de performance, de capacité de stockage et de réseau.**

Ces derniers ont le choix entre héberger directement l'infrastructure du Cloud privé sur leur propre site (« on-premise ») ou bien potentiellement dans le centre de données du fournisseur.

Exemple : OVH

LE CLOUD HYBRIDE

Un Cloud hybride combine plusieurs types d'environnements Cloud, notamment les Clouds publics et privés, et peut également inclure des infrastructures hébergées sur site.

Pour qu'un Cloud soit réellement hybride, il doit y avoir une combinaison d'au moins 2 environnements de Clouds qui échangent des informations entre eux et exécutent une série uniforme d'applications pour le compte d'un client.

Exemples :

- une combinaison d'au moins un Cloud privé et un Cloud public ;
- une combinaison d'au moins deux Clouds publics ;
- une combinaison d'au moins deux Clouds privés.

LE MULTI CLOUD

Dans ce modèle, les clients exécutent des applications à l'aide de services Cloud provenant d'au moins deux fournisseurs de services Cloud afin de créer, exploiter, accéder et sécuriser lesdites applications de manière cohérente sur l'ensemble des Clouds.

Cela permet également de minimiser la dépendance vis-à-vis d'un fournisseur.

Exemple : Anthos, la plateforme hybride de Google Cloud

Quels sont les modes d'exploitation du Cloud ?

Le Cloud permet de rendre un certain nombre de services (outils bureautiques, messagerie, comptabilité, etc.) qu'il est possible de définir en fonction des rôles et des usages à la fois des entreprises qui fournissent le service et de celles qui utilisent ledit service.

Traditionnellement, 3 grands modes existent :

Le mode IaaS (Infrastructure as a Service)

Le Cloud permet de mettre en œuvre une infrastructure virtuelle (serveur, couches de virtualisation, stockage, réseaux) sur laquelle l'entreprise utilisatrice va pouvoir héberger des systèmes d'exploitation, des serveurs et des logiciels applicatifs.

Le fournisseur Cloud gère ainsi l'infrastructure informatique uniquement alors que de son côté le client gère lui-même l'installation, la configuration, les mises à jour du système d'exploitation, des « *middlewares* » (logiciels intermédiaires) et des applications, les données, etc.

Seule l'infrastructure matérielle est donc dématérialisée.

GÉRÉS PAR LE FOURNISSEUR	Virtualisation Serveurs Stockage Réseau
GÉRÉS PAR LE CLIENT	Données Applications Environnement d'exécution Conteneurs Système d'exploitation

Le mode PasS (Platform as a Service)

Le Cloud permet de mettre en œuvre une plateforme **d'exécution de logiciels et d'applications**, sur laquelle l'entreprise utilisatrice va pouvoir installer, configurer et utiliser les applications voulues.

Avec cette solution, le fournisseur propose **l'infrastructure technique** mais également un **ensemble d'outils intégrés** qui permettent de développer des applications (système d'exploitation, base de données,...) et un serveur web. Le client lui se focalise sur le développement des applications.

GÉRÉS PAR LE FOURNISSEUR	Virtualisation Serveurs Stockage Réseau Environnement d'exécution Conteneurs Système d'exploitation
GÉRÉS PAR LE CLIENT	Données Applications

Le mode SaaS (Software as a Service)

Le Cloud fournit le **logiciel ou l'application**, regroupant les services de l'IaaS et du PaaS avec en plus, **l'installation, la maintenance et la configuration** comprises.

C'est une interface qui permet la **simple utilisation** du logiciel et ne nécessite pas de connaissance informatique ou technique au préalable.

GÉRÉS PAR LE FOURNISSEUR	Données Applications Environnement d'exécution Conteneurs Système d'exploitation Virtualisation Serveurs Stockage Réseau

En résumé :

LES MODES D'EXPLOITATION	IaaS	PaaS	SaaS
GÉRÉS PAR LE FOURNISSEUR	Virtualisation Serveurs Stockage Réseau	Virtualisation Serveurs Stockage Réseau Environnement d'exécution Conteneurs Système d'exploitation	Données Applications Environnement d'exécution Conteneurs Système d'exploitation Virtualisation Serveurs Stockage Réseau
GÉRÉS PAR LE CLIENT	Données Applications Environnement d'exécution Conteneurs Système d'exploitation	Données Applications	Données Applications Environnement d'exécution Conteneurs Système d'exploitation Virtualisation Serveurs Stockage Réseau

Quels sont les types de stockage Cloud ?

Ceux-ci sont au nombre de trois :

- **le stockage d'objets :** les objets stockent des données non structurées telles que des photos, des vidéos, des données issues du machine learning (ML), des données de capteurs, ou encore des fichiers audio. Ces données sont stockées par les objets dans le format dans lequel elles arrivent permettant ainsi de personnaliser les métadonnées de manière à faciliter l'accès aux données et leur analyse. Au lieu d'être organisés dans des fichiers ou des dossiers hiérarchisés, les objets sont conservés dans des compartiments sécurisés qui offrent une capacité de mise à l'échelle pratiquement illimitée.

- **le stockage de fichiers :** les applications utilisent très souvent un stockage basé sur les fichiers ou stockage sur fichier ce qui leur permet de stocker les données dans un dossier hiérarchique et un format de fichier.

- **le stockage de bloc :** ce stockage est utile pour les applications d'entreprise telles que les bases de données ou les systèmes de planification des ressources d'entreprise (ERP) qui nécessitent souvent un stockage dédié et à faible latence pour chaque hôte. Chaque bloc possède son propre identifiant unique pour un stockage et une récupération rapide.

Quels sont les avantages du Cloud ?

Les avantages du Cloud, pour les entreprises comme pour les particuliers, sont nombreux. Parmi ceux-ci figurent :

- **une réduction des coûts :** les structures n'ont plus besoin d'acquérir l'ensemble du matériel informatique autrefois indispensable pour leurs activités conduisant ainsi à une réduction des charges d'investissement de départ. Elles n'ont plus à obtenir des espaces de stockage ou du capital en plus lors des pics d'activité. Par ailleurs, l'absence, dans certains modèles, de maintenance et d'équipe technique dédiée permet de faire des économies. De même, le système d'abonnement offre aux clients la possibilité de ne payer que ce qu'ils consomment ;

- **la flexibilité et l'évolution des services :** en fonction des besoins, il est possible d'augmenter ou

de réduire l'utilisation des ressources informatiques proposées. En outre, les services gérés dans le Cloud sont mis à jour régulièrement ;

- la possibilité d'un **stockage quasiment illimité :** les fournisseurs **construisent** en effet sans cesse de nouveaux centres de données ;

- **un gain de temps :** le fournisseur Cloud gère lui-même un certain nombre de contraintes, telles que la maintenance, sans que le client n'ait à intervenir ;

- l'accès à des services **de très haute qualité** sans payer des coûts prohibitifs ;

- un **partage des données facilité :** tout utilisateur du cloud peut rendre disponibles ses données à un ou plusieurs autre(s) utilisateur(s) de ce cloud ;

- une **accessibilité totale :** les applications sont conçues pour être accessibles partout, depuis n'importe quel appareil connecté ;

- **la sécurisation des données :** le Cloud offre un niveau de sécurité supérieur à un système classique composé de machines physiques. En effet, dès lors que les données sont dans le Cloud un ordinateur portable perdu ou volé n'est plus un souci majeur.
  De plus, le stockage dans le cloud permet de contrôler en permanence où sont stockées les données, qui peut y avoir accès et les ressources que le client consomme ;

- **la continuité de l'activité :** les centres de données sont hautement sécurisés, protégeant ainsi les données et garantissant la continuité des activités. En cas de sinistre impactant les locaux du client (incendie par exemple), les données ne sont plus perdues.

Quels sont les inconvénients du Cloud ?

Malgré ses nombreux avantages, le Cloud Computing présente également des inconvénients, dont notamment :

- **la dépendance à Internet :** en cas de panne, l'activité entière de la structure s'en trouve perturbée ;
- **la dépendance technique par rapport aux fournisseurs Cloud:** la structure peut devenir tributaire du service proposé par un fournisseur. De plus, l'absence d'interopérabilité des systèmes peut l'empêcher de quitter son fournisseur ;
- une **perte de contrôle** du système informatique : celui-ci n'est en effet plus sous le parfait contrôle de la structure et les applications utilisées peuvent changer à tout moment, au profit d'autres plus performantes ou plus adaptées au matériel du prestataire.

Quels sont les risques particuliers en matière de protection des données personnelles ?

Outre le nécessaire équilibre à trouver entre les avantages et les inconvénients du Cloud d'un point de vue pratique, il convient également de prendre en compte les risques que pose ce système de stockage en matière de protection des données personnelles. Les données se trouvent en effet au cœur même des services offerts par le Cloud computing et comme dans tous projets informatiques, leur sécurité s'analyse en termes de **disponibilité, d'intégrité et de confidentialité des données.**

Les principaux risques sont ainsi les suivants :

- **un risque en matière de sécurité :** même si le niveau de sécurité proposé par les fournisseurs de service Cloud est élevé, les risques de pannes techniques et d'attaques informatiques ne peuvent être exclus, et ce d'autant plus que la concentration de toutes les données à un même endroit est particulièrement tentante pour les hackers. Le fait que les données transitent par Internet accroît également les risques ;
- **un risque de perte de données** dans le cadre de procédures de sauvegarde ou de stockage ;
- **un risque de fuite des données et de perte de confidentialité,** en raison du nombre de serveurs existants et de la délocalisation de ces derniers ;
- **un risque de perte de contrôle** (ou de souveraineté sur les données), notamment quant à la localisation des données et à leur assujettissement aux lois et réglementations en vigueur sur le territoire national où figurent les serveurs (exemple : des données placées dans un Cloud, avec des serveurs basés aux États-Unis). De plus, de nombreux pays ont mis en place des législations ou des pratiques, comme le Cloud Act américain, qui leur permettent d'accéder aux données hébergées sur les services Cloud ;

Le Cloud Act, qu'est-ce que c'est ?

Le Cloud Act (Clarifyng Lawful Overseas Use of Data Act) est une loi américaine qui permet aux Autorités judiciaires d'accéder aux données électroniques stockées à l'étranger par les entreprises américaines, dans le cadre de procédures pénales.

En vertu de cette loi, il est donc possible pour le gouvernement US d'accéder aux serveurs en Europe et donc à Monaco à partir du moment où la société est américaine ou si la société a une relation d'affaires avec les Etats-Unis.

Une étude publiée en août 2022 par le Ministère de la justice des Pays-Bas a conclu **que les entités européennes peuvent être soumises à cette loi extraterritoriale même si leur siège social n'est pas aux Etats-Unis dès lors qu'elles utilisent** des technologies américaines.

Elle précise même que le Cloud Act s'applique aussi quand un fournisseur de Cloud européen utilise du « *hardware* » ou un logiciel américain.

- un risque en matière de **transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat,** subordonné par la Loi à des formalités d'autorisation préalable auprès de la CCIN et à la mise en place de garanties appropriées (exemple : signature et mise en œuvre par les entités exportatrices et importatrices de données des clauses contractuelles types de la Commission européenne).

Quelles mesures prendre pour sécuriser le Cloud ?

Si le risque zéro n'existe pas, plusieurs mesures permettent toutefois de protéger les données dans le Cloud, en tenant compte de facteurs tels que le type et la sensibilité des données à protéger.

Les principales mesures sont les suivantes :

La configuration du Cloud

Un grand nombre d'atteintes à la protection des données dans le Cloud sont dues à des vulnérabilités de base, comme des erreurs de configuration.

Afin de réduire ces erreurs, il est important :

- de **modifier les paramètres établis par défaut dans leur état d'origine** ;
- de ne **jamais laisser un bucket** (conteneur) de stockage dans le Cloud ouvert ;
- d'utiliser les **commandes de sécurité** proposées par le fournisseur de services

La sécurisation des comptes

Pour éviter que des logiciels malveillants ne s'introduisent dans les systèmes d'exploitation, des **logiciels antivirus et antimalware** doivent impérativement être installés et régulièrement mis à jour.

De même, **tous les appareils** utilisés pour accéder aux données dans le Cloud doivent être sécurisés, y compris les smartphones et tablettes. En effet, si les données sont synchronisées sur plusieurs appareils, les risques que l'un d'entre eux soit compromis et affecte les autres, augmentent.

La configuration des accès aux données

Toutes les personnes au sein d'une même structure ne sont pas nécessairement habilitées à avoir accès à toutes les informations disponibles dans le Cloud. Il est donc important que les équipes IT veillent à ce que les privilèges d'administrateur ne soient accessibles qu'à ceux qui en ont réellement besoin et que les comptes desdits administrateurs soient correctement sécurisés.

De même, il convient de s'assurer que l'accès aux données soit **limité aux seuls utilisateurs dûment habilités** et que ces permissions d'accès soient supprimées ou modifiées dès lors que les utilisateurs ne sont plus habilités à accéder à une ressource car ils ont quitté la structure ou changé de fonctions.

La sécurisation des accès aux comptes

Les mots de passe permettant d'accéder aux comptes doivent être sécurisés. A cet égard, il convient d'utiliser des mots de passe uniques et complexes, régulièrement renouvelés, et de prévoir une authentification multifactorielle afin de mettre en place un barrage complémentaire en cas de divulgation dudit mot de passe.

L'utilisation d'un gestionnaire de mots de passe peut être une bonne idée afin d'attribuer des mots de passe distincts et complexes à chaque application, base de données et services, sans avoir à les mémoriser tous.

Le chiffrement des données

Parce qu'elles se déplacent d'un lieu de stockage à un autre, les données hébergées dans le Cloud risquent davantage d'être interceptées. Aussi, pour les rendre moins vulnérables, différentes façons de les chiffrer peuvent être envisagées afin que les communications ne puissent à aucun moment être accessibles aux personnes extérieures sans la clé de chiffrement :

- **le chiffrement de bout en bout** de l'ensemble des données qui sont chargées dans le Cloud (recommandé pour les informations financières, confidentielles ou commercialement sensibles) ;
- le **chiffrement des communications** avec le Cloud dans leur intégralité ;
- **le chiffrement de données particulièrement sensibles**, comme les identifiants de compte.

Il est fortement recommandé d'utiliser si possible **ses propres clés de chiffrement** et non pas celles du prestataire.
Il est également très important de gérer les clés de chiffrement de manière **sûre et sécurisée**. Il est ainsi recommandé de les conserver précieusement en dehors du Cloud, au sein même de la structure. Il peut être par ailleurs envisagé de les **mettre à jour régulièrement**.

L'installation des mises à jour de sécurité
Les cybercriminels étant toujours à l'affut des vulnérabilités, il convient de toujours installer au plus vite les mises à jour et correctifs de sécurité.

La vérification de la sécurité du fournisseur de service Cloud

Avec le recours au Cloud computing, la cybersécurité n'est plus seulement de la responsabilité du client mais dépend également du fournisseur de service. Il est donc important de se poser les questions suivantes avant de choisir son fournisseur :

- **des audits externes de sécurité sont-ils effectués régulièrement ?**
- les données relatives aux clients sont-elles segmentées logiquement et conservées séparément ?
- les données sont-elles chiffrables ? Sont-elles chiffrées ? Quelles sont les parties chiffrées ?
- quelles sont les politiques appliquées en matière de conservation des données des clients ?
- les données sont-elles bien effacées lorsqu'on quitte un service dans le Cloud ?
- comment les accès sont-ils contrôlés ?

Il convient également de lire attentivement les conditions d'utilisation (CGU) établies par le fournisseur et de s'assurer notamment que les données ne sont pas sauvegardées dans des serveurs situés dans des pays ne disposant pas d'un niveau de protection adéquat.

La mise en place de procédures internes

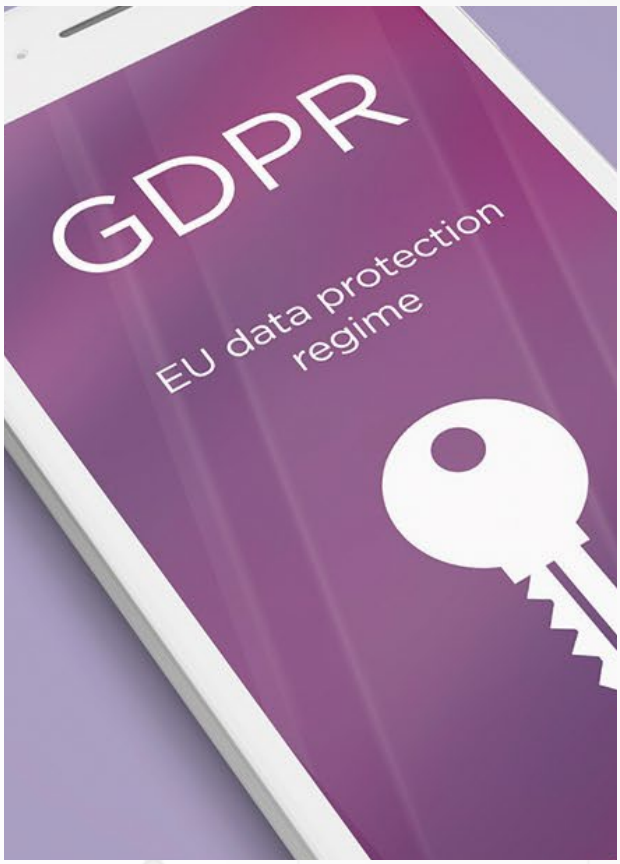
Il convient également d'établir en interne des politiques de sécurité dédiées au Cloud mais également de prévoir des formations de sensibilisation à destination des employés.

Qu'est-ce qu'un Cloud souverain ?

L'inquiétude grandissante en Europe quant à la dépendance croissante des entreprises et institutions vis-à-vis des grands fournisseurs de Cloud américains pousse de nombreux pays à promouvoir des « *Clouds de confiance* », utilisant la technologie des géants américains mais exploités par des sociétés européennes, dans des centres de données situés en Europe.

Le Cloud souverain est donc un modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de Cloud sont physiquement réalisés par une entité de droit national et en application des lois et normes nationales, afin de préserver la sécurité et la confidentialité de ces données.

C'est ainsi qu'en 2021, la Principauté de Monaco a lancé son propre Cloud souverain qui s'appuie actuellement sur deux centres de données sur le territoire national, et un centre de données de secours au Luxembourg.



LA SÉCURITÉ DES TRAITEMENTS : UNE APPROCHE GLOBALE

Aux termes de l'article 17 de la loi n° 1.165 du 23 décembre 1993 :

« *Le responsable du traitement ou son représentant est tenu de prévoir des mesures techniques et d'organisation appropriées pour protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions d'informations dans un réseau, ainsi que contre toute autre forme de traitement illicite.*

Les mesures mises en œuvre doivent assurer un niveau de sécurité adéquat au regard des risques présentés par le traitement et de la nature des données à protéger.

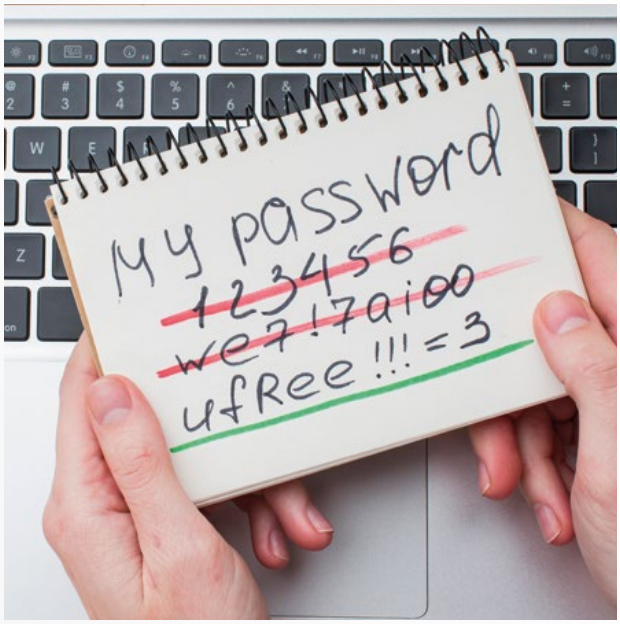
Lorsque le responsable du traitement ou son représentant a recours aux services d'un ou plusieurs prestataires, il doit s'assurer que ces derniers sont en mesure de satisfaire aux obligations prescrites aux deux précédents alinéas.

La réalisation de traitements par un prestataire doit être régie par un contrat écrit entre le prestataire et le responsable du traitement ou son représentant qui stipule notamment que le prestataire et les membres de son personnel n'agissent que sur la seule instruction du responsable du traitement ou de son représentant et que les obligations visées aux deux premiers alinéas du présent article lui incombent également.

Si le prestataire souhaite avoir recours aux services d'un ou de plusieurs sous-traitants pour l'exécution de tout ou partie des prestations prévues au contrat susvisé, les dispositions de l'alinéa précédent s'appliquent à ces derniers ».

Cette obligation de préservation des données à caractère personnel figure également à l'article 32 du RGPD.

La nécessité de protection des informations nominatives concerne tant les fichiers au format papier que ceux au format numérique.



Que veulent savoir les techniciens lors d'une analyse de dossier ?

Comment les techniciens analysent la sécurité d'un dossier ?
C'est une question que beaucoup de responsables de traitement se posent. S'il n'y a pas de formule clé en main, 6 étapes peuvent néanmoins être identifiées.

I. Etapes de l'analyse

1/ Les techniciens s'intéressent tout d'abord à la finalité du traitement qui amène à connaitre le type de données collectées. Le cycle de vie des données (flux) permet d'avoir des indications à la fois sur la donnée elle-même ainsi que sur son exploitation.

2/ Ils étudient ensuite les habilitations octroyées et la traçabilité (imputabilité possible des actions). Le schéma d'architecture technique a son importance car il aide à la compréhension du système technique déployé.

3/ Puis vient la sécurité appliquée aux données au regard de la finalité, à savoir :

- les données identifiantes, pseudonymisées, anonymisées, etc. ;
- la localisation des données : stockage interne, hébergement, cloud, etc. ;
- la sécurité logique et physique ;
- le chiffrement mis en place ;
- les sauvegardes et leurs localisations.

4/ La communication des données est également étudiée, comme par exemple :

- via les portails web ;
- par le biais d'une messagerie électronique ;
- par le biais de support(s) physique(s) (clé USB, disque dur, etc.) ;
- etc.

5/ Sans oublier, lorsque cela est le cas, tout transfert[7] de données vers un pays hors protection adéquate, avec la sécurité des données concernées par ce transfert.

6/ Enfin, il est important pour les techniciens de savoir avec quel(s) autre(s) traitement(s) le traitement étudié est rapproché et/ou interconnecté. Une justification de ce(s) rapprochements(s)/interconnexion(s) doit être fournie.

II. Cas pratique

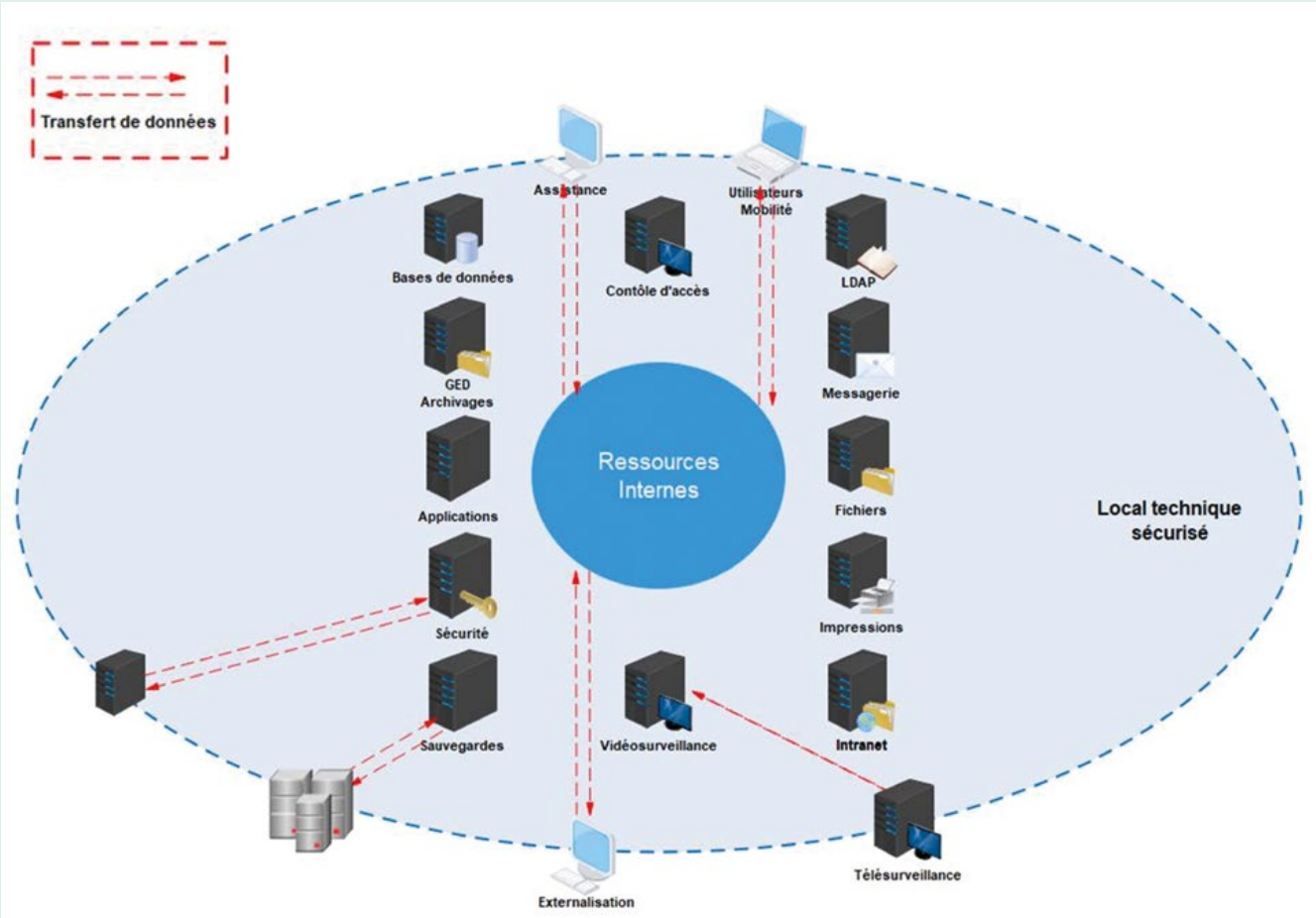
Une entreprise sise à Monaco dépose un dossier portant sur la vidéosurveillance dont le prestataire de Télésurveillance est situé en Italie.

Documents fournis :

- le formulaire de demande d'autorisation complété ;
- le schéma d'architecture technique (flux des données) ;
- le plan d'implantation des caméras.

Pour tout traitement soumis à autorisation/avis, les techniciens rédigent un rapport technique relatif à la sécurité dudit traitement. Ce rapport est présenté en Commission afin d'aider à la compréhension technique de ce traitement et à la prise de décision.

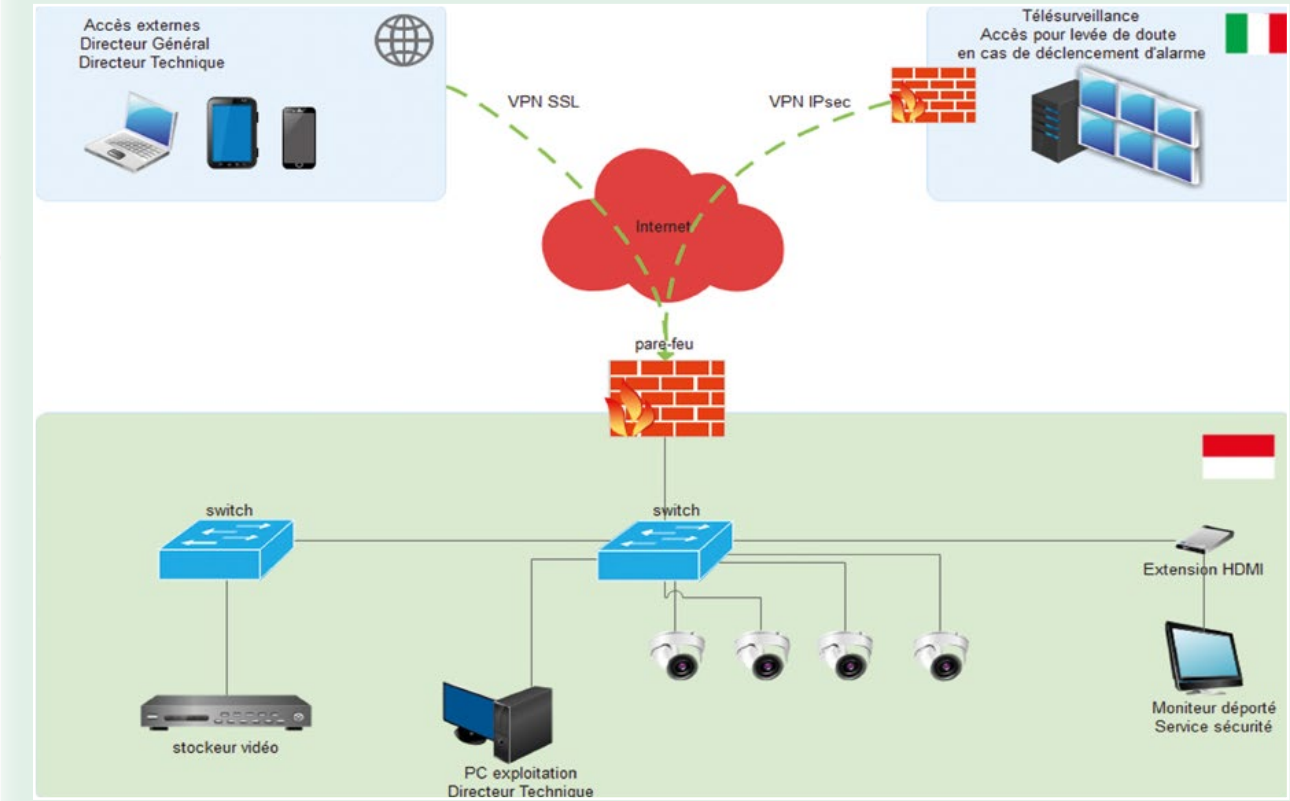
Schéma d'architecture technique globale de l'entreprise sise à Monaco



Le schéma d'architecture globale fourni par l'entreprise permet d'avoir une vision générale sur l'infrastructure technique. Cependant, afin de comprendre le traitement concerné, les techniciens ont besoin d'avoir un schéma plus précis identifiant dans cette structure ledit traitement, en l'espèce, le dispositif de vidéosurveillance.

[7] Sont également considérés comme des transferts, les accès aux informations effectués depuis un pays ne disposant pas d'un niveau de protection adéquat.

Focus sur le schéma d'architecture technique du traitement de vidéosurveillance



1/ Conformément à la procédure décrite dans la partie I, les techniciens se penchent d'abord sur la finalité qui consiste en l'installation d'un système de vidéosurveillance à des fins sécuritaires. Les quatre caméras installées sont fixes et les fonctionnalités zoom et micro ne sont pas activées. Seuls sont ainsi collectés les images, visages et silhouettes des personnes.

2/ Les techniciens analysent les habilitations ainsi que les différents types d'accès. Le schéma d'architecture technique du traitement permet notamment de vérifier la cohérence des habilitations indiquées et met aussi en évidence des accès distants sécurisés (VPN SSL) par des personnes internes à l'entreprise (le Directeur Général et le Directeur Technique).

3/ Sur la sécurité du traitement, les techniciens constatent les points suivants :

- le stockeur vidéo se situe dans un local technique fermé à clé ;
- il y a un moniteur déporté ;
- chaque personne habilitée dispose d'un identifiant et d'un mot de passe individuels pour accéder au traitement ;
- une journalisation des accès est mise en place ;
- etc.

Ils vérifient également à l'aide du plan d'implantation, l'angle de vue des caméras et, quand elles sont fournies, les captures d'écran.

4/ Les techniciens notent que l'extraction des images s'effectue sur une clé USB. Toutefois aucune procédure de chiffrement n'est prévue. Dans leur rapport technique, les techniciens demandent donc que l'extraction des images soit impérativement chiffrée sur son support de réception.

5/ A l'étude du dossier les techniciens constatent qu'il n'y a aucun transfert vers un pays hors protection adéquate. Cependant ils relèvent qu'en cas de déclenchement d'alarme, un accès aux images depuis l'Italie est effectué par le prestataire de Télésurveillance.

6/ Le responsable indique que le traitement ne fait l'objet d'aucun rapprochement ni d'interconnexion avec un autre traitement. Cependant, à l'analyse du schéma d'architecture technique, les techniciens relèvent que le prestataire de Télésurveillance agit uniquement sur déclenchement d'alarme. Il y a donc une interconnexion liée à ladite alarme qui doit être déclarée auprès de la CCIN.

Du pare-feu à l'extincteur ou de l'importance de la sécurité physique des locaux hébergeant des informations nominatives

Souvent, surtout concernant les données conservées par le biais d'un système informatique, la notion de sécurité et de conservation n'est envisagée que du point de vue strictement informatique par l'installation de divers outils (exemples pare-feu, anti-virus, chiffrement, hachage, ...).

Cependant, la sécurité des données ne se limite pas à ces aspects et doit être pensée de manière globale. Il est en effet inutile d'avoir un système sophistiqué destiné à prévenir les intrusions à distance dans un système d'information s'il est possible d'ouvrir facilement le local où se trouve le serveur informatique et de s'y connecter directement.

Lors de l'élaboration d'un plan de sécurité, la sécurisation des différents locaux est indispensable et doit être adaptée à l'entreprise et à son activité.

Il convient d'analyser les risques (externes, internes, humains, naturels, ...), leur vraisemblance (c'est-à-dire la probabilité qu'ils surviennent), la gravité de leurs conséquences éventuelles, les manières de les prévenir et si besoin de remédier à leurs effets néfastes.

Ces risques peuvent être reportés sur une cartographie des risques, et ne seront pas les mêmes selon par exemple que l'on se trouve dans un immeuble collectif divisé entre plusieurs entités ou dans un immeuble n'abritant que l'entreprise notamment en ce qui concerne la gestion des accès à l'intérieur de cet immeuble ou selon que l'entreprise reçoit ou non du public.

Un immeuble ancien ou même neuf peut ne pas avoir été conçu pour abriter tel type de société car n'offrant pas les garanties nécessaires de sécurité active et passive.

Un audit de sécurité ne doit pas négliger le volet de la protection physique des installations et le recours à un prestataire spécialisé peut être nécessaire. Dans certains cas, le recours à des bug bounty ou hackers éthiques peut permettre de tester la sécurité à « *360°* ».

De manière générale, il convient de s'assurer que l'accès aux locaux est sécurisé au moyen d'alarmes, de caméras et d'un contrôle d'accès par badge par exemple. Différentes zones doivent être définies en fonction de leur sensibilité aux risques.

Les locaux eux-mêmes doivent être conformes à la sensibilité de l'usage et au risque d'intrusion par exemple par la sécurisation des murs, fenêtres et portes d'entrée. Les accès secondaires ne doivent pas être négligés (par exemple à partir de la cave, du parking, d'un local voisin, ...).

La sécurité doit également prendre en compte outre les risques extérieurs humains, les risques naturels par des protections contre les incendies ou les dégâts des eaux, les pannes électriques, ...

Ainsi, le local abritant les serveurs informatiques, cœur de la protection informatique et par conséquent zone à haut risque d'intrusion et d'action malveillante possible, doit faire l'objet d'une attention particulière. Il doit être installé dans un lieu sécurisé anti-incendie et limitant le risque de dégâts des eaux, être correctement climatisé (il ne sert à rien d'en contrôler l'accès si on laisse la porte ouverte pour refroidir en aérant), muni d'un onduleur et maintenu dégagé de tout élément pouvant en compromettre la sécurité (on n'y entrepose pas de cartons par exemple ou de produit inflammable).

Son accès ne doit être autorisé qu'aux personnes dont la fonction implique nécessairement d'y entrer et toute personne extérieure même un prestataire lié à l'entreprise par un contrat doit y être accompagné par une personne habilitée de l'entreprise. Des badges d'accès ou des contrôles d'accès biométriques ainsi que des caméras peuvent être utilisés. Les accès doivent être tracés sur un registre même pour les personnels de l'entreprise. En cas d'intervention, la nature et la durée doivent y figurer.

Par analogie, au principe du « *besoin d'en connaître* » bien connu en matière de protection des informations nominatives, les accès aux différentes zones de l'entreprise doivent être fondés sur le « *besoin d'y accéder* ». Ainsi, un employé qui n'aurait qu'un besoin ponctuel d'accès n'a pas lieu de bénéficier d'un droit d'accès permanent et l'hôtesse d'accueil n'a pas vocation à entrer dans la salle des serveurs informatiques par exemple.

Pour les zones moins sensibles, des accès plus libres peuvent être mis en place. Cependant, une attention particulière est nécessaire afin de prévenir la circulation de personnes extérieures qui pourront par exemple être tenues de porter un badge visiteur apparent.

Un registre des visites peut être établi. Une attention particulière sera portée aux livreurs et autres prestataires qui pourraient être amenés à circuler dans les lieux.

Dans les zones non soumises à un contrôle d'accès strict, les ordinateurs fixes ou portables doivent faire l'objet de mesures de sécurité afin d'empêcher d'y accéder ou de les emporter (par exemple par l'utilisation de câbles anti-vols). Seul le matériel fourni par l'entreprise doit pouvoir être connecté au réseau de l'entreprise et les outils nomades comme les clefs USB doivent être protégés notamment du vol et chiffrés afin de réduire le risque si cela devait survenir.

Le personnel doit être sensibilité régulièrement à la sécurité globale et aux bonnes pratiques. Son attention doit être appelée sur les risques liés aux objets connectés personnels et à l'usage d'outils personnels qui peuvent être des vecteurs d'entrée de risques ou d'intrusion.

Les sauvegardes informatiques doivent être stockées dans des locaux distincts des locaux principaux. Les supports physiques de ces sauvegardes ou les documents papier sensibles doivent être placés dans des coffres forts ignifugés et étanches.

Les documents sensibles ne doivent pas être laissés sur les bureaux en dehors de la présence des personnes qui les occupent. Les open-space et les espaces de bureaux partagés nécessitent une attention et une rigueur particulière.

La gestion des codes d'accès doit faire l'objet d'une revue périodique et être régulièrement mise à jour afin notamment de priver rapidement d'accès un salarié qui quitterait l'entreprise.

Tous les intervenants extérieurs doivent être gérés selon le risque afin de prévenir tout acte malveillant.

Les copieurs multifonctions doivent également être protégés car ils stockent un grand nombre d'informations.

Les écrans affichant des données sensibles ne doivent pas être visibles de l'extérieur ou du public.

Les documents devenus inutiles mais pouvant contenir des informations sensibles doivent faire l'objet d'une destruction répondant aux normes en vigueur afin de prévenir leur reconstitution. L'inspection de vos poubelles peut en dire beaucoup sur votre entreprise et son activité.

Si vos données sont hébergées par un prestataire extérieur ou un sous-traitant, il vous appartient de vous enquérir des mesures de sécurité qu'il applique à ses locaux pour réduire le risque de divulgation ou de compromission susceptible d'engager votre responsabilité.

La sécurité commence par l'anticipation et le bon sens de chacun (comme en médecine « *mieux vaut prévenir que guérir* ») et est l'affaire de tous.

Des failles de sécurité même d'apparence mineure peuvent exposer à des conséquences dramatiques tant pour la société que pour les personnes dont les données auront été piratées.

LE CRITÈRE D'ÉTABLISSEMENT

L'application de la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée, aux traitements mis en œuvre par un responsable de traitement engendre un certain nombre de conséquences et d'obligations à la charge de ce dernier (responsabilité, formalités à régulariser auprès de la CCIN notamment...).

Aussi, la détermination du champ d'application de la Loi n° 1.165 est une étape essentielle en cas de mise en œuvre de traitements en lien avec Monaco, plus particulièrement à l'heure de la globalisation et de la banalisation de l'utilisation des nouvelles technologies, ce qui amène la CCIN à être questionnée sur ce sujet.

L'article 24 premier tiret de la Loi n° 1.165, susvisée, consacre à cet effet le critère de l' « *établissement* » et prévoit que « *les dispositions de la Loi n° 1.165 du 23 décembre 1993, modifiée, sont applicables aux traitements automatisés d'informations nominatives mis en œuvre par un responsable de traitement établi à Monaco* ».

Si la notion d'établissement n'est pas actuellement définie par le texte, il n'existe aucune exigence quant à l'implication d'une société ou d'une succursale monégasque. L'existence d'un exercice effectif, réel et stable d'activité sera en revanche un élément à prendre en considération pour retenir l'existence d'un établissement du responsable de traitement à Monaco.

Il convient toutefois de relever que la question de l'application de la Loi monégasque doit être abordée différemment s'agissant des services pour des objets connectés et des applications mobiles. Certains des traitements sont intrinsèquement liés à la vente des équipements (voitures par ex) et des options y associées et tombent dès lors dans le champ d'application de la Loi monégasque en matière de protection des informations nominatives, tandis que d'autres peuvent relever d'options ou d'outils que l'acheteur peut choisir d'activer ou utiliser ultérieurement (application mobile par exemple).

Bien qu'étant propre aux traitements entrant dans le champ d'application du RGPD, le critère de l'établissement est également consacré à l'article 3 (1) de ce Règlement pour déterminer son champ d'application territorial. Le Considérant 22 du RGPD apporte des précisions sur cette notion et mentionne notamment que « *l'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard* ».

Des exemples relatifs à la notion d'établissement se retrouvent également au sein des lignes directrices 3/2018 relatives au champ d'application territorial du RGPD adoptées par le Comité européen de la protection des données.

Il existe d'autres critères que l'établissement pour l'application de la Loi monégasque, comme il existe une application extraterritoriale du RGPD. Pour plus d'informations, une FAQ relative à l'impact du RGPD à Monaco est disponible sur le site internet de la CCIN Impact du RGPD à Monaco FAQ > CCIN

2023

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