APDP

AUTORITÉ DE **PROTECTION**
DES **DONNÉES** PERSONNELLES

RAPPORT D'ACTIVITÉ /2024

16ème rapport public

CCIN

LA CCIN ÉVOLUE ET DEVIENT L'APDP

RAPPORT D'ACTIVITÉ PUBLIÉ EN APPLICATION DE L'ARTICLE 38-20 DE LA LOI N° 1.565 RELATIVE A LA PROTECTION DES DONNÉES PERSONNELLES

L'année dernière, mon prédécesseur, Monsieur Guy Magnan, adressait l'ultime message d'un Président de la Commission de Contrôle des Informations Nominatives (CCIN).

En effet, les Lois n° 1.565 et 1.566 du 3 décembre 2024 sont venues respectivement refondre en profondeur la protection des données, et approuver la ratification du Protocole d'amendement à la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. A la CCIN s'est ainsi substituée l'Autorité de Protection des Données Personnelles (APDP).

Cette évolution majeure et structurante pour la matière en Principauté a pour objectif d'aligner le droit interne sur les plus hauts standards internationaux et européens dans un domaine toujours plus complexe, où la préservation des libertés et des droits fondamentaux des personnes est au cœur des enjeux, afin, in fine, que sa législation soit reconnue comme présentant un niveau de protection adéquat par la Commission européenne.

A cette fin, la CCIN puis l'APDP, dans les avis rendus sur les projets de textes, se sont attachées à mettre en exergue les éléments importants à prendre en compte afin de remplir les exigences du référentiel d'adéquation de l'Union européenne, dont les composantes ne se limitent pas au seul RGPD mais concernent aussi la Directive « Police/Justice » de l'Union européenne.

L'entrée en vigueur de la Loi n° 1.565 a mis fin en grande partie aux formalités préalables et c'est après avoir rendu en 2024 plus de 200 délibérations et instruit 280 dossiers de déclarations de conformité que la CCIN a tiré sa révérence.

Ce changement de paradigme a été anticipé dès le début de l'année, avec l'organisation de réunions d'information et de sensibilisation afin tout à la fois de rassurer les responsables du traitement sur leurs futures obligations, et de les accompagner dans leurs nouvelles démarches de conformité en préparant de nombreux documents et outils d'aide à la conformité. Cela s'est reflété sur la structuration même de l'Autorité, qui a procédé à une réorganisation de ses Services afin d'être en phase avec les nouvelles missions de l'APDP. Cette transformation devrait se poursuivre si les postes qu'elle a demandés pour le nécessaire renforcement de ses effectifs lui sont octroyés.

Ce changement et cette réorganisation sont allés de pair avec de nouvelles nominations au sein de la CCIN au mois de juin 2024, 4 Commissaires sur 6 n'ayant pu être renouvelés en application des dispositions qui régissaient alors cette Commission, puis, suite au vote de la Loi n° 1.565, avec un élargissement de la composition de la formation plénière qui est passée de 6 à 8 membres auxquels s'ajoutent 2 suppléants.

Concernant les anciens Membres de la CCIN je tiens ici à saluer le travail remarquable accompli durant leurs 2 mandats de 5 ans, au cours desquels ils ont été à l'écoute des entités publiques et privées de la Principauté, sans toutefois faire preuve de la moindre complaisance lorsque des atteintes à la protection des données personnelles étaient avérées.

Je souhaite également la bienvenue aux nouveaux Membres qui viennent sans aucun doute renforcer la technicité de l'APDP, avec notamment un nombre accru de magistrats, des professionnels de la santé et des experts de la société civile. Ensemble, nous ferons du « passage de relais » initié par mon prédécesseur une réussite et c'est en suivant le chemin tracé par la CCIN que l'APDP va s'attacher à accomplir ses nouvelles missions.

Aussi, dans cette année charnière qu'a été l'année 2024, je crois que nous pouvons être fiers du travail accompli. Nous sommes également conscients des enjeux à venir, portés par une nouvelle législation qui servira de socle à l'examen de la demande de reconnaissance d'adéquation de la Principauté.

Je sais que les Membres de l'APDP partagent le même souhait que moi : au-delà des textes qui nous régissent, notre Autorité démontrera, comme par le passé, l'effectivité de la protection des données en Principauté.

Robert Chanas

RAPPORT D'ACTIVITÉ APDP 2024

Sommaire

5

6

7

LA COMPOSITION DE LA **COMMISSION**

En 2024 la composition de la CCIN résultait des dispositions des articles 4 et 5 de la Loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives en application desquels 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.

Au cours de cette année, la composition de la CCIN a ainsi été modifiée au mois de juin 2024, le mandat de 4 Commissaires sur 6 ne pouvant plus être renouvelé.

Composition de la CCIN jusqu'au mois de juin 2024 :

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

Composition de la CCIN telle que résultant de l'Ordonnance Souveraine n° 10.609 du 10 juin 2024 :

De gauche à droite : Jacques Boisson, Vice-Président ; Robert Chanas, Président ; Léa Parienti, Commissaire ayant qualité de Magistrat du siège ; Jean-François Cullieyrier, Commissaire ; Jacques Rit, Commissaire ; Philippe Botto, Commissaire.

Suite à l'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024, et en application de ses dispositions finales, les Membres de la CCIN, nommés au mois de juin 2024, sont devenus Membres de l'APDP, jusqu'à publication de l'Ordonnance Souveraine procédant à la nomination des 8 Membres de cette nouvelle Autorité, qui s'est substituée à la CCIN.

La nomination des Membres de l'APDP en fonction depuis le mois de juillet 2025 est intervenue par Ordonnance Souveraine n° 11.407 du 21 juillet 2025, pour une durée de 5 ans, renouvelable une fois.

De gauche à droite : Jean-François Cullieyrier ; Jérôme Fougeras-Lavergnolle ; Florestan Bellinzona, Président de la Formation restreinte ; Robert Chanas, Président ; Jacques Boisson, Vice-Président ; Léa Parienti ; Jacques Rit ; Philippe Botto ; Serge Petit.

De gauche à droite : Jacques Boisson, Vice-Président ; Robert Chanas, Président ; Florestan Bellinzona, Président de la Formation restreinte ; Serge Petit ; Jean-François Cullieyrier ; Philippe Botto ; Jacques Rit ; Christine Bourguet.

Robert CHANAS,
Président

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.

En octobre 2022 il devient membre du Conseil d'Administration du CHPG, puis en décembre 2023 il en est nommé Vice-Président.

Il intègre la CCIN en avril 2021 sur proposition du Conseil Communal, et en est élu Président au mois de juillet 2024. Il devient Président de l'APDP à la suite de l'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024.

Au mois de juillet 2025 il est nommé Membre de l'APDP toujours sur proposition du Conseil Communal, et en est élu Président pour 5 ans lors de la réunion d'installation tenue le 28 juillet 2025.

Jacques BOISSON
Vice-Président

Licencié en Droit et titulaire d'un diplôme d'études supérieures de droit, diplômé de l'Institut d'Etudes Politiques et de l'Institut des Hautes Ecoles Internationales, et titulaire d'un Doctorat d'Etat en Droit, Jacques Boisson débute sa carrière en mars 1968 en qualité de Fonctionnaire international auprès de l'UNESCO.

D'octobre 1983 à juin 1993 il est Conseiller puis Ministre Conseiller à l'Ambassade de Monaco en France, avant d'être nommé en juillet 1993 Ambassadeur extraordinaire et plénipotentiaire, Représentant permanent de Monaco auprès des Nations Unies.

De juillet 2003 à mars 2005 il est Ambassadeur extraordinaire et plénipotentiaire à l'Ambassade de Monaco en Espagne, puis Ambassadeur extraordinaire et plénipotentiaire, représentant permanent de la Principauté auprès du Conseil de l'Europe jusqu'au mois d'octobre 2006.

Il assume ensuite, jusqu'en 2008, les hautes fonctions d'Ambassadeur extraordinaire et plénipotentiaire de la Principauté de Monaco en France, d'Ambassadeur extraordinaire et plénipotentiaire, Délégué Permanent auprès de l'UNESCO, de représentant personnel de S.A.S. le Prince Souverain auprès de l'Organisation Internationale de la Francophonie, et d'Ambassadeur extraordinaire et plénipotentiaire auprès de la Principauté d'Andorre.

En juillet 2008 il devient Secrétaire d'Etat de S.A.S. le Prince Albert II, fonctions qu'il occupera jusqu'à février 2022.

Nommé membre de la CCIN en juin 2024, sur proposition du Conseil d'Etat, il en est élu Vice-Président le 3 juillet 2024, et devient Vice-Président de l'APDP à la suite de l'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024.

En juillet 2025 il est nommé Membre de l'APDP sur proposition du Conseil d'Etat, et lors de la réunion d'installation de l'Autorité qui s'est tenue le 28 juillet 2025 Monsieur Boisson en a été élu Vice-Président pour 5 ans.

Florestan BELLINZONA

Président de la Formation restreinte

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 a été également Président de la formation correctionnelle statuant sur intérêts civils, Président de la formation correctionnelle pour mineurs et a présidé les audiences de flagrant délit ainsi qu'une partie des audiences correctionnelles.

En octobre 2020 il devient Vice-Président du Tribunal de Première Instance, puis Président du Tribunal Correctionnel depuis janvier 2025.

Désigné Membre de la CCIN en juin 2014 sur proposition du Directeur des Services Judiciaires, son mandat a été renouvelé en juin 2019, également sur proposition du Directeur des Services Judiciaires.

Au mois de juillet 2025 il est nommé Membre de l'APDP sur proposition du Premier Président de la Cour d'Appel, et assume de droit la Présidence de la Formation restreinte de l'Autorité.

Philippe BOTTO

Membre de la Formation restreinte

Titulaire d'une maîtrise en droit privé, Philippe Botto commence sa carrière en 1980 au sein du Cabinet de Monsieur Roger Orecchia, Président de l'Ordre des Experts-Comptables, en qualité de responsable juridique plus particulièrement en charge du secteur des procédures collectives d'apurement du passif.

Il intègre, en 1996, les Caisses Sociales de Monaco, en tant qu'Attaché de Direction et occupe successivement les postes de Sous-Directeur puis de Directeur Adjoint jusqu'en 2017.

Il a été membre du Comité de la Caisse de Retraite Complémentaire du Centre Hospitalier Princesse Grace de septembre 2015 à décembre 2023.

Membre du Conseil d'Administration de la Fondation Hector Otto depuis novembre 2014, il en est actuellement Vice-Président.

Il intègre la CCIN en juin 2024 sur proposition du Ministre d'Etat puis est nommé membre de l'APDP en juillet 2025, également sur proposition du Ministre d'Etat.

Lors de la séance d'installation de l'APDP tenue le 28 juillet 2025 Philippe Botto a été élu Membre de la Formation restreinte en charge des sanctions.

Jacques RIT

Membre de la Formation restreinte

Docteur en médecine, diplômé de l'université d'Aix-Marseille, Jacques Rit poursuit sa formation en qualité de chirurgien spécialiste en Orthopédie /Traumatologie au sein de l'université de Würzburg, en Allemagne.

Il débute son d'activité hospitalière au Centre Hospitalier Princesse Grâce à Monaco en 1983, dont il devient Chef du Service d'orthopédie II en 1999.

En 2006 il est nommé Chef des Services d'orthopédie I et II, et assure ces fonctions jusqu'en 2016.

Elu Conseiller National en 2003 (législature 2003-2008), puis en 2013 (législature 2013-2018) il effectue sa dernière mandature de 2018 à 2023.

En 2020 il est élu Président de la Commission Spéciale pour l'analyse de la crise Covid-19 au sein de la Haute Assemblée. A cette occasion il avait souhaité échanger avec la CCIN afin d'appréhender les enjeux de la gestion de cette crise sanitaire au regard de la préservation des droits et libertés fondamentaux des personnes. Il s'était alors fait l'écho, auprès du Gouvernement, de la nécessité d'associer la CCIN plus en amont des prises de décisions.

Nommé Membre de la CCIN sur proposition du Conseil National en juin 2024, il devient Membre de l'APDP à la suite de l'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024.

Au mois de juillet 2025 il est nommé Membre de l'APDP sur proposition du Conseil National, et lors de la réunion d'installation de l'Autorité qui s'est tenue le 28 juillet 2025 Jacques Rit a été élu aux fins de siéger dans la Formation restreinte en charge des sanctions.

Jean-François CULLIEYRIER

Membre titulaire

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 a assuré le Secrétariat, la Vice-Présidence et les fonctions de Trésorier de 1977 jusqu'en 2023.

En 2001, il devient Administrateur, Directeur Central d'HSBC Private Bank, et depuis 2018 il est 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.

Ancien Membre du Conseil de la Couronne il siège actuellement au Tribunal du Travail, 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 proposition du Conseil Economique et Social dont il a été membre à partir de 1989 puis Président de la Section financière jusqu'en 2012.

Renouvelé en qualité de Membre de la CCIN en juin 2024, il est nommé Membre de l'APDP en juillet 2025, sur proposition du Conseil Economique, Social et Environnemental.

Serge PETIT
Membre titulaire

Diplômé en droit public et sciences politiques, Serge Petit débute sa carrière dans l'enseignement universitaire, puis assure les fonctions de Secrétaire Général de l'Institut Régional d'Administration de Lille.

Il intègre la Magistrature en 1987 d'abord en qualité de Juge d'Instance de Douai, puis de Juge au Tribunal de Grande Instance de Paris, dont il est Juge d'Instruction jusqu'en 1994.

Conseiller référendaire à la Cour de Cassation de 1995 à 2003, il intègre ensuite la Cour des Comptes, d'abord en qualité de Conseiller Rapporteur, puis de Chargé de Mission au Cabinet du Premier Président, avant d'être nommé Secrétaire Général, chargé plus particulièrement de la réforme du Code des juridictions financières et de la mise en place ainsi que du suivi de la réforme de la Cour des Comptes et de la Cour de Discipline Budgétaire et Financière. Il participera également à la Mission d'audit et de contrôle de la Cour Européenne des Droits de l'Homme.

En 2004 il devient Directeur des études du Médiateur de la République française, et en 2007 il est nommé Avocat Général à la Cour de Cassation, fonctions qu'il occupe jusqu'en 2016. Parallèlement il intervient en qualité d'expert auprès du Conseil de l'Europe au sein de la Commission Européenne pour l'Efficacité de la Justice.

Avocat Général honoraire à la Cour de Cassation depuis mai 2016, il est Conseiller à la Cour de Révision depuis novembre 2014.

Nommé Membre de l'APDP en juillet 2025 sur proposition du Premier Président de la Cour de Révision, il sera en charge des droits d'accès indirects pour le compte de l'Autorité, ainsi que des missions d'investigations en lien avec les traitements « *Police/Justice* ».

Christine BOURGUET
Membre titulaire

Après l'obtention d'un Doctorat en Médecine Générale à l'Université de Nice, Christine Bourguet exerce la médecine générale pendant 3 ans avant d'intégrer par concours un poste de Médecin Conseil auprès de la Caisse d'Assurance Maladie en 1995.

En 2005 elle choisit de s'orienter vers la médecine du travail et valide cette spécialité en 2008.

Après 8 années d'exercice au sein du Centre Santé et Sécurité au Travail à Menton, elle décide d'enrichir son expérience en intégrant l'Office de la Médecine du Travail (OMT) à Monaco.

Intéressée par le milieu marin, elle débute une formation en médecine hyperbare en 2017 afin de suivre les plongeurs professionnels qui vont intervenir en grand nombre sur le chantier d'extension en mer de la Principauté.

Depuis 2020 elle exerce son métier de Médecin du Travail à mi-temps afin de se consacrer également à la coordination de l'équipe médicale et pluridisciplinaire au sein de l'OMT.

Le Docteur Christine Bourguet intègre l'APDP en juillet 2025, sur proposition du Comité de la Santé Publique, en qualité de Membre qualifié dans le domaine de la santé.

Jérôme FOUGERAS LAVERGNOLLE

Membre suppléant

Titulaire d'une Maîtrise de Droit privé option Carrières Judiciaires, Jérôme Fougeras Lavergnolle intègre l'Ecole Nationale de la Magistrature de Bordeaux en 2000 et effectue son stage juridictionnel au sein du Tribunal de Grande Instance de Marseille.

Il débute sa carrière à Monaco, d'abord en qualité de Juge suppléant pendant 1 an, avant d'être nommé en 2003 Juge au Tribunal de Première Instance et désigné aux fonctions de Juge tutélaire jusqu'en 2011.

De 2008 à 2011 il exerce également les fonctions de Juge d'instruction, puis est nommé Premier Juge en 2011, jusqu'en 2018. Parallèlement il siège de 2014 à 2018 au sein du Haut Conseil de la Magistrature.

En 2014 il assume la présidence du Tribunal Correctionnel et en 2018 il est également nommé Vice-Président du Tribunal de Première Instance, fonctions qu'il occupe jusqu'au mois de décembre 2024.

De 2006 à 2023 il siège au Comité Consultatif des Juges Européens du Conseil de l'Europe, en qualité de représentant de la Principauté.

En janvier 2025 il est nommé Conseiller à la Cour d'Appel.

Jérôme Fougeras Lavergnolle intègre l'APDP au mois de juillet 2025, en qualité de Membre suppléant désigné sur proposition du Premier Président de la Cour d'Appel et aura à assurer la Présidence de la Formation restreinte en charge des sanctions en cas de déport du Membre titulaire.

Léa PARIENTI

Membre suppléant

Titulaire d'une Maîtrise en droit Carrières judiciaires, Léa Parienti intègre ensuite l'Ecole Nationale de la Magistrature.

Après avoir exercé durant 14 années en France en qualité de Juge des enfants, de Magistrat à l'Administration centrale de la justice, de Juge aux affaires familiales puis de Juge d'instance, elle intègre la Magistrature monégasque en 2014.

Elle y exerce successivement les fonctions de Magistrat référendaire, de Juge au Tribunal de Première Instance, et de Premier Juge depuis avril 2021.

Léa Parienti est actuellement Juge tutélaire et préside la Chambre du Conseil du TPI.

En sa qualité de Magistrat du siège elle est nommée Membre de la CCIN en juin 2024, sur proposition du Directeur des Services Judiciaires – Secrétaire d'Etat à la Justice, et devient Membre de l'APDP à la suite de l'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024.

Au mois de juillet 2025 elle est désignée Membre suppléant de l'APDP sur proposition du Premier Président de la Cour de Révision et aura à assurer les contrôles sur les traitements « *Police/ Justice* » ainsi que les exercices de droits d'accès indirect en cas de déport du Membre titulaire.


RAPPORT
D'ACTIVITÉ
/2024
16ème rapport public

1

DE LA CCIN À L'APDP 31 ANNÉES D'ÉVOLUTION

Le 28 novembre 2024 la Loi substituant l'APDP à la CCIN a été votée. L'occasion de faire le point sur l'évolution de cette Commission au fil des années, et les nouvelles missions de l'APDP !

La protection des données en 3 années clés :

1993 : création de la CCIN : Loi n° 1.165 du 23 décembre 1993 réglementant les traitements d'informations nominatives

Cette création a résulté du constat que l'utilisation de procédés électroniques permettait la collecte, le regroupement, et le partage d'informations nominatives de manière bien plus rapide que les procédés non automatisés, tant pour la gestion des Services Publics que pour la conduite des affaires privées.

L'informatique était entendue au sens de la Loi n° 1.165 adoptée en 1993 comme étant « *des méthodes qui doivent être utilisées pour transformer l'information, des mécanismes qui permettent de réaliser ces transformations, des modes de communication les plus appropriés entre les utilisateurs et les techniciens en la matière, ainsi que des moyens matériels qui doivent être mis en œuvre. En elle-même l'informatique est neutre, mais par les applications qui peuvent en être faites, elle peut être facteur de libération ou facteur d'asservissement.* »

Aussi est apparue la nécessité d'encadrer l'utilisation des procédés automatisés de collecte et de traitement de ces informations, en vue d'assurer la protection des libertés et droits fondamentaux des personnes concernées.

C'est ainsi qu'est née la CCIN, qui était alors instituée auprès du Ministre d'Etat. Elle était composée de 3 Membres titulaires et de 3 Membres suppléants, et son Président était nommé par Ordonnance Souveraine.

Ses missions étaient alors de recevoir les déclarations de mise en œuvre de traitements par des personnes de droit privé, et de donner un avis lorsque les traitements étaient mis en œuvre par des personnes morales de droit public.

Dès l'origine la CCIN pouvait être saisie de réclamations par les particuliers, et avait la possibilité de procéder à des contrôles de régularité. Les irrégularités qu'elle relevait devaient toutefois être signalées au Ministre d'Etat, auquel il incombait d'émettre des mises en demeure, et de saisir les juridictions lorsque les irrégularités émanaient de personnes physiques ou morales de droit privé, ou de prendre toute mesure utile afin de faire cesser les irrégularités à l'encontre de services dépendant d'une personne morale de droit public.

Cette Loi initiale conférait également un certain nombre de droits aux personnes concernées : droit à l'information, droit d'accès, de rectification, ..., et des dispositions instauraient la possibilité pour les ascendants, les descendants jusqu'au second degré, ou le conjoint survivant d'une personne décédée, d'exercer ces mêmes droits pour les informations relatives à cette personne.

Elle prévoyait des sanctions pénales en cas de non-respect de ces nouvelles dispositions légales, dont des peines de prison pouvant aller jusqu'à 1 an.

« *L'informatique ne connaissant pas de frontières* », cette Loi était de portée extraterritoriale en ce que les principes de respect des droits et libertés des personnes concernées s'appliquaient également aux traitements automatisés d'informations nominatives mis en œuvre à l'étranger et accessibles à Monaco.

2008 : la CCIN devient une Autorité Administrative Indépendante : Loi n° 1.353 du 4 décembre 2008 modifiant la Loi n° 1.165 du 23 décembre 1993

En 2008, la Principauté a souhaité ratifier la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ainsi que son Protocole additionnel concernant les Autorités de contrôle et les flux transfrontières de données.

Dans le prolongement de la Loi autorisant ces ratifications, la Loi n° 1.353 du 4 décembre 2008 a modifié de manière substantielle la Loi n° 1.165 afin de rendre conforme le droit interne à ce nouveau corpus juridique international dont Monaco souhaitait être Partie.

Le double objectif de cette réforme :

« *- créer les conditions propres à assurer l'essor de l'économie numérique en sécurisant les relations juridiques établies au travers de communications électroniques ;*

- renforcer la protection des droits fondamentaux de la personne compte tenu des risques encourus du fait de l'intensification de l'usage de moyens technologiques de plus en plus performants. »

En outre, d'ores et déjà, la Principauté souhaitait rapprocher sa législation de la législation européenne telle qu'elle résultait de la Directive n° 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, afin de pouvoir bénéficier d'une reconnaissance d'adéquation de sa législation par l'Union européenne (UE), facilitant ainsi les échanges de données avec les Pays européens.

Afin de se conformer à ces nouveaux standards internationaux et européens, la première modification structurelle a été d'ériger la CCIN en authentique Autorité Administrative Indépendante (AAI), au sens de la Convention 108, de son Protocole additionnel, et du Règlement de l'Union européenne. Sur ce point, la doctrine gouvernementale de l'époque considérait que des AAI ne pouvaient être créées à Monaco que lorsque cela « *est requis par l'exécution des engagements internationaux de la Principauté, et dans ce cas elles ne peuvent être investies que des compétences strictement nécessaires à la satisfaction desdites engagements* », en l'espèce la Convention 108 du Conseil de l'Europe et son Protocole additionnel.

En sa qualité d'AAI, la CCIN n'est plus instituée « *auprès du Ministre d'Etat* » mais doit à l'inverse exercer ses activités « *en toute indépendance* », et ses Membres ne doivent recevoir « *d'instruction d'aucune autorité* ». De nouveaux pouvoirs lui ont été conférés (ester en Justice, dénoncer au Procureur Général les infractions, délivrer des autorisations administratives). Le Président de la CCIN a alors été investi du pouvoir de mettre en demeure un responsable de traitement de se conformer à ses obligations, et de le sanctionner par le biais d'un avertissement.

Par ailleurs, les formalités préalables ont été étoffées, et un nouveau régime d'autorisation préalable a été instauré pour les entités privées, concernant les traitements mis en œuvre à des fins de surveillance (vidéosurveillance par ex), ou contenant des données biométriques, ou portant sur des soupçons d'activités illicites (traitements en matière de lutte contre le blanchiment de capitaux notamment).

Les transferts d'informations nominatives vers des Pays n'assurant pas un niveau de protection adéquat devaient également faire l'objet d'une autorisation préalable de la CCIN.

La Commission devait désormais être consultée par le Ministre d'Etat sur des projets de textes en lien avec le traitement d'informations nominatives.

Le Président de la Commission était élu par ses pairs, et l'indépendance budgétaire de la CCIN a été accrue.

La CCIN a également été chargée d'exercer les droits d'accès indirects au sein de traitements mis en œuvre à des fins de sécurité publique, et en matière de lutte contre le blanchiment de capitaux.

Comme par le passé, elle pouvait effectuer des contrôles sur place afin de vérifier la régularité des traitements. Cependant, le 25 octobre 2013, le Tribunal Suprême a considéré que les dispositions de la Loi n° 1.165, issues de la réforme législative de 2008, et relatives aux missions de contrôle sur place, portaient « *au principe d'inviolabilité du domicile, consacré par l'article 21 de la Constitution, une atteinte qui ne peut être regardée comme proportionnée au but d'intérêt général poursuivi par la Loi n° 1.165* ». Ainsi, les pouvoirs d'investigation de la CCIN ont été jugés contraires à la Constitution, privant la Commission de la possibilité d'effectuer des contrôles.

Les pouvoirs d'investigation des Autorités de protection des données personnelles constituant un élément fondamental dans le processus de reconnaissance d'adéquation conduit sous l'égide de la Commission européenne, la demande qu'avait introduite la Principauté en 2009 afin de bénéficier d'une décision d'adéquation a alors été suspendue.

Afin de remédier à cette situation, la Loi n° 1.420 du 1er décembre 2015 est venue rétablir les pouvoirs d'investigation de la CCIN, tout en les entourant de garanties destinées à préserver les droits des entités contrôlées dont notamment : le droit d'opposition ouvert lors de contrôles effectués au sein de locaux professionnels privés, l'autorisation judicaire préalable en cas de contrôle faisant suite à la réception d'une plainte, l'introduction de recours juridictionnels à différents stades de la procédure de contrôle.

Cette réforme législative de 2015 a été également l'occasion d'introduire la possibilité pour le Président de la CCIN de rendre publics les avertissements et les mises en demeure, là aussi avec des recours ouverts aux personnes sanctionnées qui en sont l'objet.

A la suite de la réintroduction des pouvoirs d'investigation de la CCIN, le Gouvernement s'est rapproché de la Commission européenne afin de l'en informer, pour qu'elle poursuive l'examen de la demande d'adéquation de la Principauté.

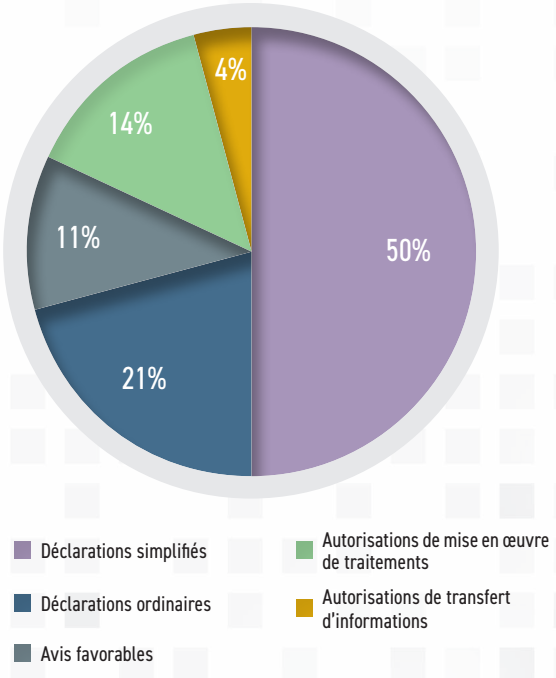
En réponse les Services de la Commission européenne ont toutefois fait valoir que désormais, les examens des demandes d'adéquation prenaient en compte le Règlement Général sur la Protection des Données (RGPD), ainsi que la Jurisprudence de la Cour de Justice de l'Union Européenne en matière d'accès par les Autorités publiques aux données personnelles, notamment pour des raisons de sécurité nationale.
Aussi, il incombait à Monaco d'adapter son droit interne en prenant en compte notamment ce nouveau texte européen. Les travaux en ce sens ont débuté en 2018.

Bilan de l'activité de la CCIN

De 2009 à 2024 la CCIN a délivré :

- 3.528 récépissés de déclaration simplifiée de conformité
- 1.492 récépissés de déclaration ordinaire
- 777 avis favorables à la mise en œuvre de traitements du secteur public et assimilé
- 1.034 autorisations de mise en œuvre de traitements par des organismes privés
- 286 autorisations de transferts d'informations vers des Pays ne disposant pas d'un niveau de protection adéquat
- Elle a émis 68 avis sur des projets de texte
- Elle a exercé 30 droits d'accès indirects
- Instruit 378 plaintes dont 104 demandes de déréférencements / suppressions de contenus numériques
- Mené 53 missions de contrôle
- Prononcé 10 avertissements et 29 mises en demeure
- Transmis 16 dossiers au Procureur Général

Les formalités préalables de 2009 à 2024



2024 : de la CCIN à l'APDP : un changement de paradigme : Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles

Instituée par la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles, l'Autorité de Protection des Données Personnelles se substitue à la Commission de Contrôle des Informations Nominatives.

L'entrée en vigueur de la nouvelle législation résulte du souhait de mettre à niveau le droit interne au regard des standards internationaux résultant désormais de la Convention 108 modernisée du Conseil de l'Europe, et de l'entrée en application du RGPD de l'Union européenne.

L'objectif de cette réforme est que la Principauté bénéficie d'une reconnaissance d'adéquation de sa législation par la Commission européenne afin de fluidifier les échanges de données, notamment avec les pays de l'UE. Le référentiel d'adéquation de l'UE portant également sur les traitements dits « *Police/Justice* », la Loi n° 1.565 y consacre une partie spécifique.

Aussi, dès le mois de juin 2025, la Principauté a officiellement formalisé sa demande d'adéquation auprès de l'Union européenne.

Cette nouvelle Loi a une **portée à la fois territoriale et extraterritoriale** puisqu'elle s'applique aux traitements de données à caractère personnel, automatisés en tout ou partie, ainsi qu'aux traitements non automatisés de données contenues ou appelées à figurer dans des fichiers :

- **mis en œuvre par un responsable du traitement ou un sous-traitant établi à Monaco**, que le traitement ait lieu à Monaco ou non ;
- **relatifs à des personnes concernées se trouvant sur le territoire de la Principauté et mis en œuvre par un responsable du traitement** ou un **sous-traitant** établi hors du territoire de la Principauté lorsque les activités de traitement sont liées à l'offre de biens ou de services ou au suivi du comportement de ces personnes.

Comme par le passé, la Loi ne s'applique en revanche pas aux traitements mis en œuvre par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

Exemple : le stockage de photos de famille ou de photos privées sur un ordinateur.

- le principe de l**imitation des finalités** ;
- le principe de **minimisation** des données ;
- le principe d'**exactitude des données** ;
- le principe de **limitation de la conservation des données** ;
- le principe de **sécurité**.

Point 3 : Le renforcement des droits des personnes concernées

La personne concernée bénéficie désormais de 8 droits lui permettant de garder la maîtrise des données la concernant, à savoir :

- le droit à l'**information** (articles 10 et 11) ;
- le droit d'**accès** à ses données (article 12) ;
- le droit de **rectification** de ses données (article 13) ;
- le droit à l'**effacement** de ses données (article 14) ;
- le droit à la **limitation** du traitement (article 15) ;
- le droit d'**opposition** au traitement de ses données (article 17) ;
- le droit à la **portabilité** (article 18) ;
- le droit de **ne pas faire l'objet d'une décision produisant des effets juridiques à son égard ou l'affectant de manière significative**, prise sur le seul fondement d'un traitement automatisé, y compris le profilage (article 19).

La nouvelle législation relative à la protection des données personnelles en 9 points :

Point 1 : Une nouvelle Autorité avec des pouvoirs renforcés

Les informations nominatives deviennent des **données personnelles** et la **Commission de Contrôle des Informations Nominatives (CCIN)** est remplacée par **l'Autorité de Protection des Données Personnelles (APDP).**

Conformément à la Convention 108+, les pouvoirs de la nouvelle Autorité de protection des données sont renforcés, en particulier dans le domaine des sanctions.

Les missions de l'APDP sont au nombre de 20 et sont détaillées à l'article 38 de la nouvelle législation.

Elles peuvent se résumer comme suit :

- Protéger et défendre les droits des personnes concernées
- Accompagner et aider à la conformité
- Veiller au respect des obligations légales
- Sanctionner en cas de manquement à la Loi

L'APDP peut également désormais être saisie pour avis sur des propositions ou des projets de lois par le Président du Conseil National. De plus, les avis rendus sur des projets de texte peuvent être publiés, ce qui n'était pas le cas auparavant.

Point 2 : Les principes essentiels en matière de protection des données personnelles

La Loi reprend dans son article **4 les 6 grands principes** prévus par les textes européens, à savoir :

- le principe de licéité, de **loyauté et de transparence** ;

Point 4 : Les obligations du responsable du traitement

La nouvelle Loi **supprime un très grand nombre de formalités préalables** en vertu du nouveau **principe de responsabilisation.**

A cet égard, elle intègre **les outils de mise en conformité des traitements** applicables aux responsables du traitement, à savoir :

- la désignation dans certains cas d'un **représentant** en Principauté ou, à défaut, au sein d'un Etat membre de l'Union européenne (article 25) ;
- la désignation dans certains cas d'un **Délégué à la Protection des Données** (articles 28, 29 et 30) ;
- la tenue d'un **registre des activités de traitement** (article 27) ;
- le respect de la protection des données dès la **conception et par défaut** (article 23) ;
- l'obligation de notifier les **violations de données** susceptibles d'engendrer un risque pour les droits et libertés des personnes concernées (article 32) ;
- l'obligation de réaliser une **analyse d'impact**, pour les traitements entraînant un **risque élevé** pour les droits et libertés des personnes concernées (articles 35 et 36) ;
- la possibilité d'adhérer à un **code de conduite** (article 33) ;
- la possibilité d'obtenir une **certification** (article 34).

Point 5 : Suppression de la plupart des formalités préalables

Dans une logique de **responsabilisation des responsables du traitement**, un très grand nombre de traitements ne font désormais plus l'objet de formalités préalables auprès de l'APDP (exemples : gestion des fichiers clients, gestion des obligations en matière de lutte anti blanchiment (LAB)).

Des exceptions demeurent toutefois (article 58 de la Loi).

Sont ainsi soumis à **l'avis préalable** de l'APDP, trois catégories de traitements présentant une **sensibilité particulière** :

- les traitements mis en œuvre à des fins de **prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales,** y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
- les traitements portant sur des **données génétiques** ou **biométriques** nécessaires à **l'authentification** ou au **contrôle** de l'identité des personnes ;

Pour ces deux premières catégories de traitements, ne sont concernées par cette obligation de formalités préalables que les Autorités administratives et judiciaires compétentes dans le cadre exclusif des missions qui leur sont légalement conférées.

- les traitements ayant pour fin la **recherche dans le domaine de la santé.**

Est par ailleurs soumis à l'autorisation préalable de l'APDP, le transfert de données à destination d'un pays, d'un territoire ou d'une organisation internationale n'assurant pas un niveau de protection adéquat lorsque :

- des **garanties appropriées n'ont pas été mises en place,** et
- **aucune des dérogations prévues à** l'article 99 de la Loi ne s'applique, et
- les **4 conditions prévues** par le chiffre 3 de l'article 99 **ne sont pas réunies**

Cas particulier des systèmes de vidéosurveillance :

L'article 85 de la Loi prévoit en outre que les systèmes de vidéosurveillance installés dans les **lieux non ouverts au public** sont **portés, sans délai, à la connaissance de l'APDP.**

Au sens de l'exposé des motifs, un lieu non ouvert au public est « *par exemple un lieu privé, (domicile, garage...) ou des locaux à usage professionnel tels que les bureaux ou les entrepôts* ».

S'agissant plus particulièrement des domiciles, ou tout autre lieu affecté à un usage personnel ou domestique, la déclaration auprès de l'APDP doit être effectuée **uniquement si des personnes extérieures au cercle familial ou amical interviennent au domicile ex : gens de maison, aides à domicile.**

Les systèmes de vidéosurveillance installés dans des **lieux ouverts au public ou filmant les abords de voie publique, d'espaces ouverts au public ou à la circulation du public**, restent quant à eux soumis à l'autorisation préalable du Ministre d'Etat.

Au sens de l'exposé des motifs, les lieux ouverts au public sont par exemple « *un restaurant, une galerie commerciale, ou un guichet d'administration* ».

Enfin, il est important de souligner que dans certains cas, le responsable du traitement devra également « *procéder à une analyse d'impact comme notamment lorsque la surveillance s'exerce à grande échelle, par exemple, dans un centre commercial ou dans une galerie marchande* ».

Point 6 : Un encadrement du recours à la sous-traitance

Dès lors qu'un responsable du traitement a recours à un sous-traitant, ce dernier doit présenter les **garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées** de manière **à assurer la protection des données personnelles et le respect des droits des personnes concernées.**

Tout recours à un sous-traitant doit être régi par un contrat dont les clauses minimales sont prévues à l'article 26.

Le sous-traitant est par ailleurs soumis aux obligations suivantes :

- la désignation dans certains cas d'un **représentant** en Principauté ou, à défaut, au sein d'un Etat membre de l'Union européenne ;
- la désignation dans certains cas d'un **Délégué à la Protection des Données** ;
- la tenue d'un **registre des activités de traitement.**

Point 7 : Une obligation de sécurité renforcée des données et de leur traitement

Tout responsable du traitement ou sous-traitant doit mettre en place des **mesures techniques et organisationnelles appropriées** afin de garantir un **niveau de sécurité adapté aux risques** pour les droits et libertés des personnes concernées.

L'adoption de ces mesures nécessite une analyse permettant d'identifier les risques puis de déterminer leur niveau de probabilité et de gravité.

Point 8 : Des sanctions renforcées

Le Président de l'APDP peut signaler à un responsable du traitement ou à un sous-traitant que les opérations envisagées sont susceptibles de ne pas être conformes. Il peut également prononcer une mise en demeure de mettre fin aux irregularités.

La Formation restreinte de l'APDP peut pour sa part prononcer une des sanctions suivantes en vertu de l'article 51 :

un **avertissement ;**

- une **obligation de mise en conformité** du traitement ou de **satisfaire aux demandes de la personne concernée**, qui peut être assortie d'une astreinte pouvant aller jusqu'à **10.000 € / jour de retard calendaire ;**
- une **limitation temporaire ou définitive du traitement ;**
- un **retrait de l'agrément** ou l'injonction de refuser une certification ou de retirer la certification accordée par l'organisme agréé ;
- un **retrait de la certification** délivrée par l'APDP ;
- une suspension totale ou partielle de la **décision d'approbation des règles d'entreprises contraignantes ;**
- une **suspension des flux de données** adressées à un destinataire situé à l'étranger ;
- une **amende administrative** (articles 53 et 54 de la Loi) pouvant aller jusqu'à 5.000.000 € (ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent) ou 10.000.000 € (ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent).

Point 9 : Un encadrement des transferts de données

Si l'article 97 pose le principe selon lequel **tout transfert de données personnelles hors de la Principauté** peut s'effectuer **sans aucune formalité préalable** dès lors que la législation ou la réglementation des données personnelles du pays, du territoire ou de l'organisation internationale destinataire dispose d'un **niveau de protection adéquat,** les articles 98 et 99 encadrent strictement tous les autres transferts.

Ainsi tout transfert vers un pays ne disposant pas d'un niveau de protection adéquat ne peut s'effectuer que si des **garanties appropriées** ont été mises en place par le responsable du traitement ou, lorsque cela n'est pas le cas, si une des dérogations expressément prévues par la Loi s'applique.

Si aucune de ces exigences n'est remplie, une autorisation **préalable de transfer**t doit être demandée à l'APDP conformément à l'article 100.

S'agissant des formalités préalables initiées sous l'empire de la Loi n° 1.165, les dispositions finales de la Loi n° 1.565 du 3 décembre 2024 prévoient que l'APDP informe les responsables de traitement de la nature de leurs nouvelles obligations.

Conformément à ces dispositions, 113 courriers ont été adressés par l'APDP, portant sur plus de 150 dossiers en cours d'instruction lors de l'entrée en vigueur de la Loi n° 1.565.

2

LES MISSIONS ET LE FONCTIONNEMENT DE L'APDP

Formation plénière 8 membres

Les missions de l'APDP sont nombreuses et ressortent de l'article 38 de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles.

Une nouveauté de la Loi n° 1.565 : l'APDP est composée au total de 3 Formations, et les missions de l'APDP sont réparties au sein de ces 3 Formations.

Les différentes Formations de l'APDP

La Formation plénière

La Formation plénière est composée de la totalité des 8 Membres de l'APDP, et ne peut valablement délibérer que si plus de la moitié de ses Membres assistent à la séance.

Ses décisions sont adoptées à la majorité absolue des suffrages exprimés, ou la majorité absolue des Membres composant l'APDP lorsqu'elles portent sur l'élection du Président et du Vice-Président de l'Autorité, la désignation des Membres de la Formation restreinte et l'adoption du Règlement Intérieur.

Une mission d'information et de sensibilisation

Au travers de la publication :

- de ses délibérations portant avis sur la mise en œuvre de traitements ;
- de ses délibérations portant avis sur des projets de textes législatifs ou règlementaires ;
- du rapport annuel d'activité ;
- de ses recommandations et lignes directrices sur des sujets spécifiques ;
- de communiqués et de fiches pratiques sur son site Internet www.apdp.mc ;
- de publications sur sa page LinkedIn ;
- de codes de conduite et de clauses contractuelles types préalablement approuvés par elle.

L'examen des formalités préalables

- Outre les missions de sensibilisation, d'information et de conseil, l'APDP est également chargée d'émettre des avis relatifs à la mise en œuvre de certains traitements :

- les traitements dits « *Police/Justice* », dont notamment ceux comportant des données génétiques ou biométriques ;
- les traitements relatifs à la recherche dans le domaine de la santé, qui sont désormais tous soumis à avis préalable de l'APDP.

Une nouveauté : l'exclusion du champ de compétence de l'APDP des traitements intéressant la sûreté publique et la sécurité nationale, régis par les articles 9 à 15 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale. Ces traitements relèvent désormais de la Commission Spéciale de Sécurité Nationale (CSSN).

Jusqu'à l'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024, ces traitements entraient dans le champ de compétence de la CCIN. Lorsque le Gouvernement a manifesté le souhait d'exclure ces traitements de l'examen et du contrôle de l'Autorité de Protection des Données Personnelles, la CCIN, consultée alors sur le projet de Loi, a rappelé à de nombreuses reprises qu'afin de répondre aux standards internationaux, et d'être en phase avec le référentiel d'adéquation de l'UE, il était indispensable que la CSSN dispose de l'ensemble des attributs d'une Autorité Administrative Indépendante au sens européen.

L'APDP a également pour mission d'autoriser les transferts vers des Pays non adéquats, lorsque ces transferts ne disposent pas de garanties appropriées légalement définies, ou n'entrent pas dans les dérogations légales.

Les nouvelles missions de l'APDP

En lien avec les nouvelles obligations des responsables du traitement, l'APDP est désormais chargée notamment d'émettre un avis sur les analyses d'impact présentant un risque élevé pour les droits des personnes concernées, de valider des codes de conduite sectoriels, de délivrer des certifications et des agréments aux organismes de certification.

Chargée de recevoir les notifications de violations de données, elle peut contraindre un responsable du traitement à informer les personnes concernées, en cas de risque élevé pour leurs droits et libertés.

En matière de transfert vers des pays ne disposant pas d'un niveau de protection adéquat, elle doit adopter et publier des clauses contractuelles types.

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

Régi par l'article 74 de la Loi n° 1.565, le droit d'accès indirect permet à toute personne concernée de saisir l'APDP afin qu'elle accède, pour son compte, aux données personnelles 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 de l'Autorité Monégasque de Sécurité Financière.

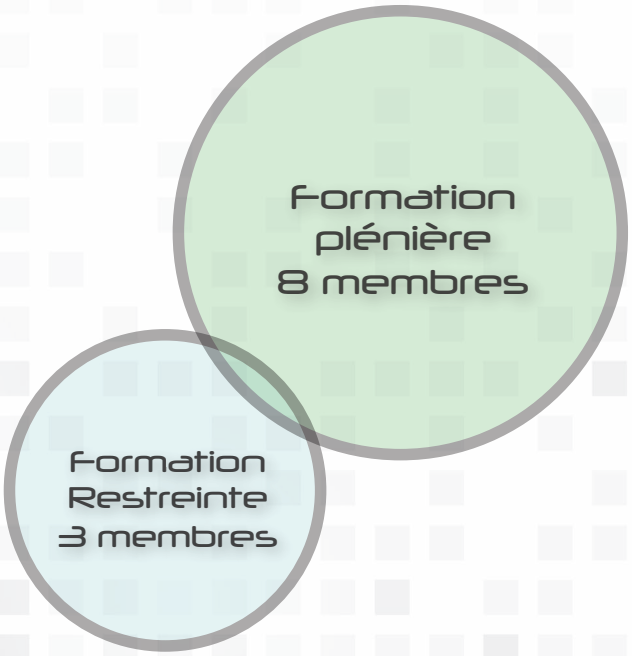
Si la formulation de l'article 74 de la Loi n° 1.565 reprend celle de l'article 15-1 de la Loi n° 1.165, en prévoyant que l'APDP effectue « *toutes les vérifications* », les articles 59 et 60 de l'Ordonnance Souveraine n° 11.327 du 10 juillet 2025 portant application de la Loi n° 1.565 introduisent toutefois une procédure écrite entre l'APDP et le responsable du traitement, et ce n'est qu'à l'issue de cette procédure écrite que l'APDP pourra se rendre dans les locaux du responsable du traitement afin de prendre connaissance des documents qu'il aura mis à sa disposition.

La Formation restreinte

Présidée par le Magistrat du siège nommé sur proposition du Premier Président de la Cour d'Appel, ou par son suppléant, elle comprend 2 Membres de l'APDP élus en son sein, pour la durée de leur mandat.

Ne peuvent siéger au sein de la Formation restreinte le Président et le Vice-Président de l'APDP, ainsi que le Magistrat désigné sur proposition du Premier Président de la Cour de Révision, dans la mesure où celui-ci a pour mission d'effectuer les contrôles sur les traitements dits « *Police/Justice* ».

La Formation restreinte ne peut valablement délibérer qu'en présence de la totalité de ses Membres.



Cette Formation est en charge de prononcer les sanctions à l'encontre des responsables du traitement ou des sous-traitants qui ne respectent pas les obligations de la Loi n° 1.565.

Conformément au souhait qu'avait émis la CCIN, les situations de conflit d'intérêt sont prévues, afin d'éviter toute partialité potentielle dans les décisions prises par la Formation restreinte.

La Loi n° 1.565 fixe également les règles de procédure applicables afin de garantir les droits des mis en cause : respect du contradictoire, délais de convocation, modalités d'audition des mis en cause et de leurs conseils, fixation des délais de réponse, modalités de notification des décisions, ...

Dans le prolongement du RGPD, et afin de répondre aux standards internationaux en matière de protection des données personnelles, les sanctions administratives ont été considérablement étoffées, notamment par le biais d'amendes administratives pouvant atteindre 10 M€ ou 4 % du chiffre d'affaires annuel mondial, en fonction de la gravité des manquements.

Constituent notamment les manquements les plus graves : le traitement de données sensibles hors les cas légalement prévus, le non-respect des droits des personnes concernées, la communication de renseignements ou de documents inexacts aux personnes concernées ou à celles chargées d'effectuer les vérifications ou investigations, ...

La Formation contrôle

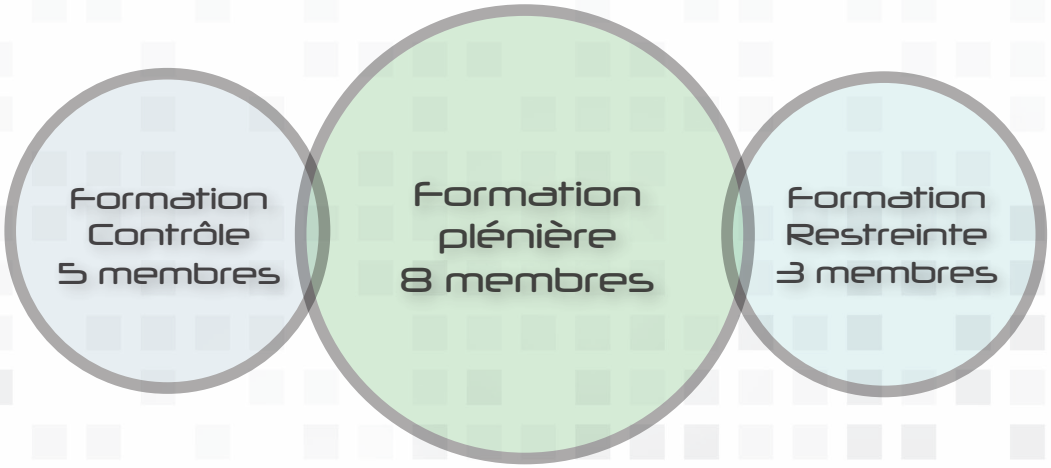
Chargée de décider de faire procéder à une mission d'investigation, la Formation « *contrôle* » prend ses décisions hors la présence des Membres de la Formation restreinte. Elle ne peut valablement délibérer que si au moins 3 de ses Membres assistent à la séance, et les décisions sont adoptées à la majorité absolue des suffrages exprimés.

Chaque décision de procéder à un contrôle fait l'objet d'une délibération qui précise le nom et l'adresse de la personne physique ou morale concernée, l'objet de la mission, ainsi que, le cas échéant, la possibilité de recourir à des experts spécialisés dans un domaine particulier.

Cette délibération doit être visée dans la Lettre de Mission délivrée par le Président de l'Autorité aux Agents en charge d'effectuer le contrôle concerné.

Désormais encadrés par les articles 46 à 49 de la Loi n° 1.565, ces pouvoirs sont similaires à ceux dont disposait la CCIN, et prévoient 2 cas de figure distincts.

L'article 48 définit le cadre des investigations « *préventives* », que l'APDP mène de sa propre initiative. Dans ce cas, a été prévue la possibilité pour les responsables de locaux professionnels de faire valoir leur droit de s'opposer aux opérations d'investigation ; celles-ci ne pourront alors se dérouler que sur autori-



sation 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 49 prévoit une procédure spécifique lorsqu'il existe des raisons de soupçonner que la mise en œuvre de traitements n'est pas conforme à la Loi sur la protection des données personnelles, 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.

L'APDP peut également décider de mener des contrôles en ligne, ou sur convocation.

Afin d'éviter toute situation de conflit d'intérêt, il est désormais prévu que nul Agent de l'APDP, ou investigateur, ne peut être désigné pour procéder aux vérifications et investigations auprès d'une entité s'il détient ou a détenu au cours des 2 années précédant la vérification ou l'investigation, un intérêt direct ou indirect, a exercé des fonctions ou une activité professionnelle ou détenu un mandat au sein de ladite entité.

Les ressources humaines et financières

En 2024 la CCIN a été dotée d'un budget total de 1.808.000,00 € contre 1.774.100,00 € en 2023, se répartissant comme suit :

- 1.100.000,00 € au titre des crédits de fonctionnement, dont la moitié est consacrée aux frais liés à ses locaux, et principalement à leur location ;
- 708.000,00 € au titre des dépenses salariales.

L'augmentation de la dotation liée à ses frais de fonctionnement résulte, outre la réévaluation du montant de son loyer, de la refonte intégrale de son site Internet dans la perspective de l'entrée en vigueur de la nouvelle législation relative à la protection des données personnelles, qui est intervenue en fin d'année 2024.

Pour remplir ses missions, l'APDP 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 sont composés d'un Chargé de Mission spécialisé en ingénierie et en sécurité des systèmes, de six juristes ayant des domaines de compétences spécifiques, d'un informaticien et de deux Agents administratifs.

6 Agents du Secrétariat Général sont assermentés afin de procéder aux missions de contrôle.

Le Secrétariat Général sert d'intermédiaire entre les responsables de traitements, les personnes concernées et l'APDP. Ils sont amenés à participer à de nombreuses réunions de travail, et à effectuer des présentations sur des thématiques spécifiques en fonction de l'auditoire.

L'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles a donné lieu à une réorganisation du Secrétariat Général, en prenant en compte les nouvelles missions de l'APDP :

La Division conformité et international a notamment en charge :

- l'instruction et le suivi des notifications des violations de données personnelles ;
- d'assurer le relais avec les Délégués à la Protection des Données : tenue à jour de la liste des DPD déclarés auprès de l'APDP, vérification de la régularité des désignations, animation du réseau des DPD ;
- la mise à disposition de documentations et d'outils d'aide à la conformité sur le site Internet ;
- l'examen des analyses d'impact soumises à l'avis de l'APDP ;
- l'instruction des demandes d'avis en matière de recherches dans le domaine de la santé ;
- le suivi de la conformité de l'APDP ;
- la représentation de l'APDP à l'international et la participation à des Groupes de travail.

La Division contrôles et régalien assume plus particulièrement :

- l'instruction et le suivi des plaintes dont notamment l'ensemble des demandes de suppression de contenus numériques ;
- l'exercice et le suivi des droits d'accès indirects ;
- la réalisation et le suivi des contrôles ;
- la préparation des documents de saisine de la Formation restreinte en charge des sanctions ;
- l'examen des projets de textes soumis à l'avis de l'APDP ;
- l'analyse des demandes d'avis des traitements « *Police/Justice* ».

La Division contentieux et sanctions a pour missions :

- d'organiser les réunions de la Formation restreinte et d'en assurer le secrétariat ;
- d'effectuer le suivi des procédures de sanctions ;
- de veiller au respect des règles de procédure devant la Formation restreinte ;
- de s'assurer de la bonne exécution des sanctions prononcées par la Formation restreinte ;
- de gérer l'ensemble de l'activité contentieuse de l'APDP.

La Division technique a des missions spécifiques telles que :

- l'évolution et le maintien à niveau du système d'information de l'APDP ;
- l'évaluation et l'analyse des nouveaux outils et services numériques afin d'en apprécier la conformité ;
- l'analyse des différentes solutions d'intelligence artificielle.

Elle intervient également de manière transverse, en collaboration avec les Divisions juridiques dans le cadre principalement :

- des analyses et du suivi des notifications de violations de données personnelles ;
- de l'instruction des plaintes en lien avec des outils numériques ;
- de l'analyse des dossiers de demandes d'avis portant sur la mise en œuvre de traitements afin d'en apprécier les mesures de sécurité ;
- du développement et de l'implémentation d'outils d'aide à la conformité sur le site Internet de l'APDP ;
- de la réalisation de missions de contrôle.

La Division administrative quant à elle assure :

- l'élaboration du budget de l'APDP et son suivi ;
- la gestion de l'ensemble des demandes et dossiers soumis à l'APDP ;
- la préparation et l'organisation des réunions de l'APDP ainsi que la gestion des suites à y donner ;
- le Secrétariat des Divisions et de l'APDP ;
- l'accueil physique et téléphonique ;
- l'organisation des déplacements.

3

LA DEFENSE DES DROITS DES PERSONNES CONCERNEES

NB : dans le présent chapitre il est mentionné la CCIN et non l'APDP dans la mesure où les dossiers auxquels il est fait référence ont été instruits avant l'entrée en vigueur de la Loi n° 1.565 ayant substitué l'APDP à la CCIN.

Il est à noter que depuis l'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles les traitements qui auront été soumis à formalité préalable seront désormais mis à disposition du public sur le site Internet de l'APDP.

Les consultations du répertoire public des traitements

- En 2024 le répertoire public des traitements a été consulté à 3 reprises :
- Par 2 Cabinets conseil pour faire le point sur les traitements déclarés par au total 3 clients : 2 de ces clients avaient effectué les formalités préalables auprès de la CCIN, ce qui n'était pas le cas du 3ème. La situation de cette entité a été régularisée à la suite de la consultation du répertoire.
- Par 1 salarié pour vérifier si le système de vidéosurveillance mis en œuvre sur son lieu de travail avait fait l'objet d'une autorisation préalable de la CCIN. Ayant constaté que tel n'était pas le cas, une plainte a été déposée auprès de la CCIN, qui a donné lieu à un contrôle la même année.

Les plaintes

37 plaintes ont été adressées à la Commission en 2024, en diminution par rapport à l'année précédente au cours de laquelle elle avait été saisie par 49 personnes. Cette diminution s'explique par le fait que souvent les personnes concernées prennent d'abord l'attache de l'APDP afin d'obtenir des renseignements pour résoudre elles-mêmes leurs difficultés, et ce n'est qu'en cas d'échec qu'elles saisissent officiellement l'Autorité d'une plainte.

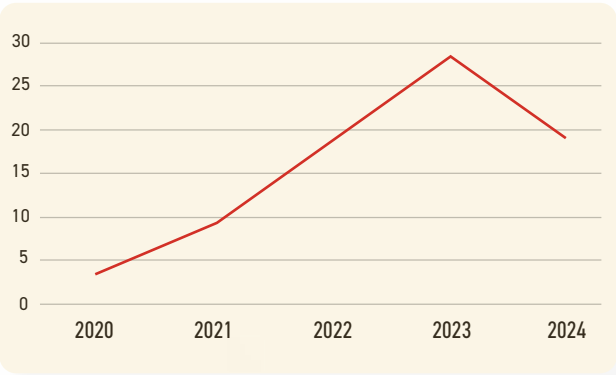
Evolution du nombre annuel de plaintes :

2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
51	17	11	15	13	15	24	19	28	41	49	37

Les plaintes liées à l'utilisation des réseaux sociaux

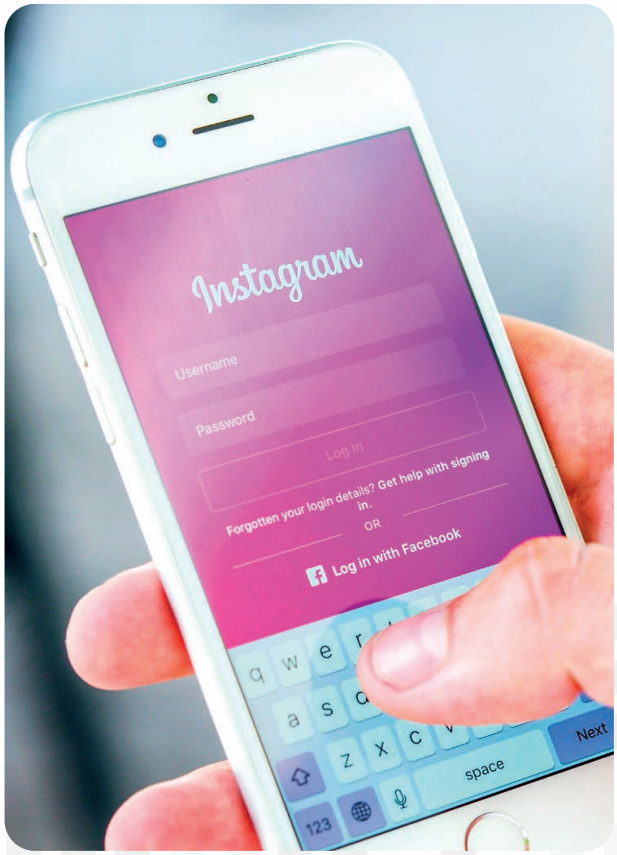
21 plaintes portant sur la suppression de contenus publiés en ligne ont été déposées en 2024, en légère baisse par rapport à l'année 2023 (28 plaintes).

Evolution des demandes depuis 2020

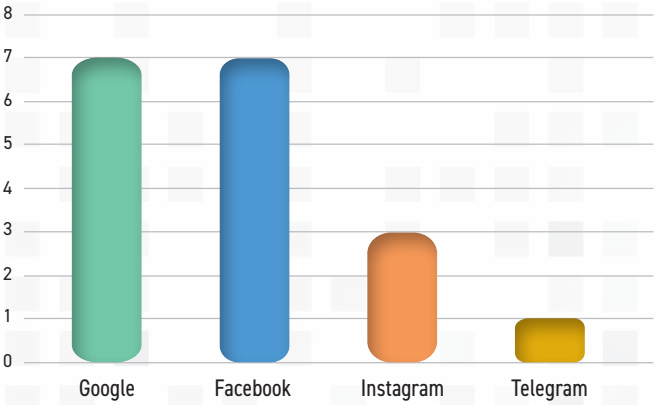


Sur ces 21 plaintes, 5 ont été classées sans suite en raison d'une absence de précision de la part des plaignants. Ces derniers n'ont notamment pas transmis les liens hypertextes menant vers les contenus en cause et un plaignant ne résidait pas en Principauté.

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 et la suppression de faux comptes.

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

Par ailleurs, il a été constaté une augmentation des saisines relatives à des contenus diffamatoires ou frauduleux. Ainsi, la Commission a agi dans le cadre de 3 plaintes pour solliciter le déréférencement de liens URL auprès du moteur de recherche Google :

- deux personnalités publiques de la Principauté ont vu leur image être utilisée pour la promotion d'une « *plateforme d'investissement* ». Les contenus dont le déréférencement a été sollicité avaient été diffusés via plusieurs publications sponsorisées sur Facebook. Ces publications comportaient en effet un lien URL menant sur un site Internet usurpant l'identité visuelle du journal Monaco-Matin dans le but d'inciter les internautes à croire les propos à caractère diffamatoire qui y étaient tenus. Ainsi, ces pages Internet induisaient les résidents monégasques en erreur puisque pensant qu'il s'agissait du véritable site d'information Monaco-Matin, ils pouvaient croire les informations diffusées et dès lors communiquer leurs données personnelles afin de s'inscrire sur la prétendue « *plateforme d'investissement* ».

Dans le cadre du traitement de cette demande, il a été constaté qu'il peut être très difficile de déréférencer certains contenus en raison de l'absence d'indexation au moment de la publication dudit contenu.

Ainsi, après avoir relevé que les pages Internet concernées n'apparaissaient pas dans les résultats Google après une recherche avec le nom et le prénom des personnes concernées, y compris lorsqu'à ces informations était joint le nom de la « plateforme d'investissement », la Commission a sollicité en plus du déréférencement auprès de Google la suppression des publications Facebook diffusant les liens.

Toutefois, la CCIN n'a pas réussi à obtenir gain de cause auprès du réseau social au motif que les publications sponsorisées ne sont pas référencées. En effet, il n'est pas possible de les identifier en communiquant le lien menant vers la publication dont s'agit ni de retrouver le compte à l'origine de celle-ci.

- une personne physique a contacté la Commission pour solliciter le déréférencement d'un site Internet frauduleux utilisant comme nom de domaine ses nom et prénom. En effet, lorsqu'une recherche était effectuée sur Google avec ces informations, un site Internet de prêt-à-porter féminin apparaissait dans les résultats. Ce site usurpait en réalité l'identité visuelle d'une véritable marque de prêt-à-porter puisque une fois sur le site le nom de la marque était indiqué avec seulement pour différence le lien URL qui lui reprenait le nom et prénom de la plaignante. Suite à l'intervention de la CCIN le moteur de recherche nous a indiqué avoir procédé au déréférencement du site.
- une société de yachting a contacté la Commission pour obtenir le déréférencement d'un site Internet

qui republiait ses propres annonces de vente et de location de bateaux ainsi que les photos et les descriptifs disponibles sur son propre site Internet. De plus, des brokers/employés de la société de yachting apparaissaient sur ce site avec leurs noms, prénoms, photos ainsi que leurs coordonnées professionnelles. Dans le cadre de cette demande, il n'a pas été possible d'obtenir le déréférencement du lien auprès de Google. En effet ce dernier a indiqué que « *Le site semble avoir une activité légale et utiliser majoritairement des données sur des personnes morales, raison pour laquelle le déréférencement de tout le nom de domaine serait disproportionné. Les données sur les yachts, donc des données non-personnelles sont les plus représentées sur le site* ».

Deux plaignantes ont saisi l'Autorité pour demander la suppression d'un avis calomnieux Google My Business qui mentionnait leurs noms et prénoms accompagnés de propos à caractère diffamatoire. Après l'intervention de l'APDP, Google a supprimé l'avis en cause au motif qu'il ne respectait pas les règles d'utilisation.

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.

Par ailleurs 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.

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

Enfin, la CCIN a traité pour la première fois une demande de suppression d'un contenu publié sur le réseau Telegram.

Il a ainsi été constaté qu'en raison du fonctionnement de cette plateforme de messagerie instantanée, qui permet la création de groupes de discussions parfois comportant plusieurs milliers de membres, il est très difficile d'obtenir la suppression des publications concernées.

En effet, l'identification du contenu en cause est très difficile pour le réseau qui sollicite la communication du lien vers la publication en cause ainsi que le lien et le nom du groupe sur lequel cette dernière est intervenue.

Les caméras de vidéosurveillance

L'exploitation de dispositifs de vidéosurveillance est devenue au fil des ans un domaine qui suscite de plus en plus d'inquiétude pour les personnes concernées, ce qui explique le nombre croissant de plaintes en lien avec des caméras de vidéosurveillance.

6 plaintes ont été reçues en 2024, dont 4 concernaient l'exploitation de caméras sur le lieu de travail. 3 d'entre elles ont donné lieu à des contrôles au cours de cette même année (voir *infra* : les investigations).

La quatrième plainte portait sur des caméras installées au sein d'établissements accueillant des enfants, dont le positionnement laissait à penser qu'elles pouvaient donner lieu à une surveillance des personnels. Ce dossier avait donné lieu quelques mois auparavant à une visite des Agents de la CCIN dans la perspective d'informer le responsable de traitement de ce qui était possible, ou non, en termes d'implantation. Les dossiers relatifs à ces caméras ont été reçus courant d'année 2024, et ont donné lieu à une réunion avec les représentants des établissements afin d'examiner l'implantation et le champ de toutes les caméras. Il a ainsi été convenu de repositionner certaines d'entre elles afin de ne pas filmer notamment les espaces de détente mis à la disposition des enfants, ainsi que les salles de réunion et les lieux dédiés aux repas. Par ailleurs au sein de l'un des établissements concernés par la plainte, les caméras avaient d'ores et déjà été validées par la CCIN en prenant des mesures spécifiques destinées à préserver la vie privée des enfants et des personnels, dont notamment l'activation de certaines caméras uniquement la nuit et les jours de fermeture de l'établissement.

La CCIN a également été saisie d'une plainte relative à des caméras qui auraient été installées dans une copropriété, dont le gardien avait dit aux occupants de l'immeuble qu'il avait des images sur lesquelles ils apparaissaient en train de fumer dans les parties communes. L'instruction de cette plainte a permis de constater qu'une seule caméra, au fil de l'eau sans enregistrement des images, était installée à l'entrée du parking. Constatant que le champ de cette caméra permettait de visionner une partie de la voie publique, il a été demandé de la repositionner, ce qui a été fait.

Enfin, un dispositif de vidéosurveillance installé au sein d'un domicile a donné lieu en fin d'année 2024 à une plainte de voisins qui redoutaient que les caméras permettent de filmer l'intérieur de leurs locaux, ainsi que la voie publique. Ils craignaient également que ce dispositif enregistre leurs conversations. S'agissant des caméras installées dans les domiciles, et même si la Loi n° 1.165 relative à la protection des informations nominatives excluait de son champ d'application les traitements « *mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques* », la CCIN avait adopté une recommandation par laquelle elle demandait que ces caméras lui soient déclarées lorsque des personnels de maison ou des prestataires non occasionnels intervenaient au sein des domiciles. En effet la présence de caméras pouvait alors permettre de surveiller le travail de ces tiers, ce que la CCIN interdisait.

La Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles connait la même exclusion de son champ d'application, mais est venue conforter cette position, et son exposé des motifs précise que « *Si le dispositif de vidéosurveillance est utilisé en dehors de la sphère strictement privée, c'est-à-dire lorsque des personnes extérieures au cercle familial ou amical interviennent au domicile comme par exemple, des gens de maison ou des aides à domicile, le particulier en tant qu'employeur doit respecter les dispositions de la présente section [Section IV Traitements relatifs à la vidéosurveillance]* ».

Aussi, conformément à l'article 85 de la Loi n° 1.565, il a été demandé à cette personne de s'acquitter de l'obligation qui était la sienne de porter, sans délai, à la connaissance de l'APDP l'existence dudit dispositif en cas d'intervention de tiers au sein de son domicile, ce qui a été fait. Dans le cadre de l'instruction de cette plainte, l'APDP a constaté qu'un dispositif occultant était installé afin de ne filmer que la propriété privée concernée, et qu'aucun dispositif permettant l'écoute ou l'enregistrement des conversations n'était actif.

L'utilisation d'outils numériques en lien avec le milieu professionnel

Domaine de saisine en progression au fil des ans, l'utilisation d'outils numériques sur le lieu de travail a donné lieu à 4 plaintes en 2024.

3 d'entre elles ont concerné la non désactivation d'adresses email nominatives en cas de départ définitif de salariés.

Dans le premier cas, la situation a été régularisée dès la première démarche auprès du responsable de traitement : la boîte email nominative a été désactivée, et un message automatique a été implémenté afin

d'informer les expéditeurs d'email que leur interlocuteur habituel ne travaillait plus au sein de l'entité, et étaient invités à contacter un nouvel interlocuteur. De plus l'adresse email nominative de l'ancien salarié n'avait pas été utilisée pour répondre, en son nom, à des messages.

En revanche les éléments transmis à la CCIN à l'appui des 2 autres plaintes, qui concernaient le même responsable de traitement, démontraient que les adresses email nominatives d'anciens salariés étaient utilisées après leur départ, afin de répondre à des sollicitations. Compte tenu de ces éléments, la CCIN a effectué un contrôle sur place en 2024 (voir infra les investigations).

La quatrième plainte portait sur l'éventuelle exploitation de différents outils, potentiellement utilisés à des fins de surveillance des salariés. En fin d'année cette plainte était toujours en cours d'instruction afin de déterminer son périmètre exact, après que les premiers éléments de vérification aient permis d'écarter certains points sur lesquels portaient la saisine de la Commission.

La rectification et l'accès aux données

Le droit de rectification

Dans cette affaire le plaignant avait constaté qu'un responsable de traitement, situé en France, lui opposait des éléments dont l'origine provenait d'un responsable de traitement implanté à Monaco.

Après s'être assurée de la légalité de ces transmissions d'informations nominatives, la CCIN s'est rapprochée de l'entité située à Monaco, et a constaté que les données transmises ne correspondaient pas, pour partie, aux éléments qui étaient opposés au plaignant. Aussi celui-ci a été en mesure d'obtenir la rectification de sa situation auprès du responsable de traitement français.

La récupération de données privées

A la suite de son licenciement, un plaignant a saisi la CCIN en fin d'année 2024 afin de pouvoir récupérer ses données personnelles, accessibles depuis l'ordinateur portable professionnel qui lui avait été confié dans le cadre de son activité salariée. A défaut de restitution de cet ordinateur lors de son départ, l'ancien employeur avait activé des mesures de sécurité irréversibles et lancé un processus de verrouillage et d'effacement de l'ordinateur à distance, afin d'éviter que l'ancien salarié puisse accéder aux données professionnelles gérées par son ancien employeur.

En fin d'année 2024 ce dossier était toujours en cours d'examen. En effet plusieurs solutions alternatives ont été proposées au plaignant, qui n'y a pas donné suite.

Le traitement des données

L'anonymisation des décisions accessibles sur Légimonaco

L'anonymisation insuffisante d'une décision publiée sur le site Internet Légimonaco a conduit à la saisine de la CCIN. La décision publiée sur ce site mentionnait en effet la dénomination sociale de l'entité au sein de laquelle le plaignant exerçait des fonctions de direction, permettant aisément de connaître son identité.

L'intervention de la CCIN auprès de l'exploitant de ce site Internet a permis très rapidement de faire rectifier cette situation.

La divulgation et la collecte des données

- une première affaire a concerné une question de divulgation potentielle de données, sans qu'il y ait eu pour autant de problématique spécifique identifiée. La CCIN est intervenue auprès du responsable de traitement pour qu'un rappel des règles soit effectué auprès de ses salariés.
- la question de la licéité de collectes de données a donné lieu à 2 plaintes.

Dans le premier cas il était demandé à des Agents publics assumant des fonctions spécifiques, de communiquer certaines catégories de données personnelles. Les réunions avec les représentants du responsable de traitement ont permis à la CCIN d'échanger avec eux sur la justification de ces nouvelles obligations, ainsi que sur leurs contours et leurs modalités. Il a été convenu de la mise en place de modalités permettant d'assurer la confidentialité des données recueillies, ainsi que l'élargissement des moyens mis en œuvre afin, à l'avenir, que les personnes manifestant leur candidature pour occuper les postes concernés, soient préalablement informées des obligations déclaratives qui pèseront sur elles en cas de recrutement.

La seconde affaire a résulté de la publication d'un article de presse mentionnant la collecte de données relatives aux plaignants, à leur insu. Il était toutefois précisé que les documents incriminés avaient été détruits, et que des plaintes sur ce sujet avaient été déposées auprès du Procureur Général. En outre, la personne à l'origine de cette collecte n'exerçait plus d'activité professionnelle, ce qui aurait dû conduire à effectuer un contrôle au sein de son domicile, ce que la CCIN ne pouvait pas faire à cette date.

Aussi la Commission, constatant que ce dossier avait d'ores et déjà fait l'objet d'une plainte pénale, a souligné que ses moyens d'actions les plus pertinents, à l'époque, consistaient à saisir le Procureur Général, ce qui avait déjà été fait par les plaignants.

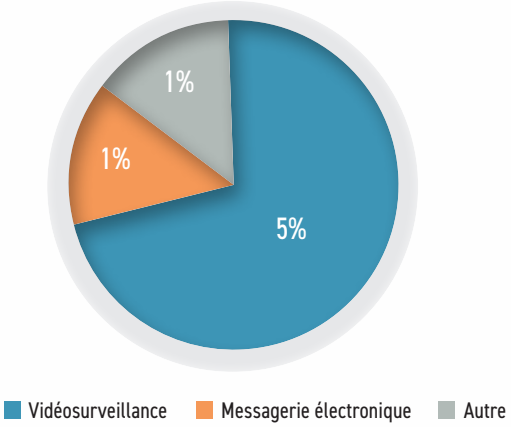
En application de l'article 18-1 de la Loi n° 1.165, introduit en 2015, la CCIN ne pouvait pas effectuer de contrôle au sein d'un domicile privé. Désormais, l'article 49 de la Loi n° 1.565 a rétabli cette possibilité, tout en l'encadrant : l'accès au domicile privé ne peut s'effectuer que si l'APDP a des raisons de soupçonner l'existence de non conformités, et uniquement sur autorisation préalable du Président du Tribunal de Première Instance, sans possibilité d'exercice d'un droit d'opposition.

Les investigations

Au cours de l'année 2024 la CCIN a effectué 7 investigations sur place : 6 d'entre elles ont fait suite à des signalements et la Commission s'est autosaisie à une reprise.

La vidéosurveillance sur le lieu de travail a été une nouvelle fois la thématique principale des contrôles.

Investigations 2024
Répartition par thématiques



Investigations relatives aux systèmes de vidéosurveillance

Les 5 investigations diligentées au cours de l'année concernaient des entités du secteur privé, étant précisé que seule l'une d'entre elles avait effectué des formalités préalables auprès de la CCIN pour obtenir une autorisation de mise en œuvre.

Il a résulté de l'ensemble des investigations menées au sein de ces entités (dont certaines disposaient de plusieurs établissements en Principauté qui ont tous été vérifiés), l'utilisation de plusieurs caméras dont l'orientation permettait de filmer les postes de travail des salariés, les écrans d'ordinateurs ainsi que les clients. De plus, il a été constaté que certaines caméras étaient dotées de détecteurs de mouvements qui déclenchaient la capture d'image ainsi que de fonctionnalités zoom, ce qui, en fonction de leur utilisation, peut constituer un risque important d'atteinte à la vie privée des salariés et des clients.

En outre, il a été relevé que la majorité des différents responsables des locaux disposaient d'un accès en continu aux images du système à l'aide d'applications installées sur leurs smartphones, ce qui est susceptible de conduire à un contrôle permanent et continu des personnes concernées.

Par ailleurs lors de l'ensemble de ces contrôles des manquements à l'information des personnes concernées ont été constatés. Ainsi, même si des affichages informant de l'existence d'un système de vidéosurveillance pouvaient être présents à l'entrée des locaux des différents établissements, il a été constaté que ces derniers n'étaient conformes ni aux dispositions de l'article 14 de la Loi n° 1.165, ni à la recommandation n° 2010-13 de la CCIN relative aux dispositifs de vidéosurveillance mis en œuvre par les personnes physiques ou morales de droit privé.

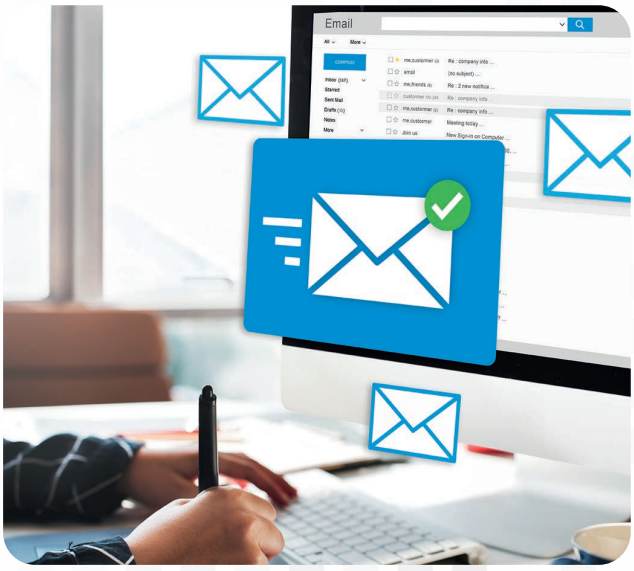
Enfin, il a été relevé lors de 2 contrôles un manquement à l'article 17-1 de la Loi n° 1.165 relatif aux mesures techniques à mettre en œuvre pour garantir la sécurité et l'intégrité des informations nominatives traitées. Ainsi, une entité n'était pas en mesure de déterminer nominativement la liste des personnes autorisées à avoir accès au traitement, tandis que la seconde n'avait implémenté aucune journalisation des accès.

Un de ces contrôles a conduit le Président de la CCIN à adopter une mesure correctrice dès l'année 2024 (voir infra : les mesures correctrices et sanctions). L'analyse des suites à donner aux autres contrôles se poursuivra en 2025.

Investigation relative à la messagerie électronique professionnelle

La Commission a diligenté pour la première fois en fin d'année 2024 une investigation portant sur l'exploitation d'un outil de messagerie électronique au sein d'une entité privée de la place.

La mission d'investigation avait notamment pour objet de vérifier les modalités d'exploitation de cet outil afin de déterminer si elle s'effectuait à des fins de surveillance permanente et inopportune des personnes concernées, ainsi que de vérifier les pratiques/procédures mises en place en cas de départ définitif d'un salarié.



Il a tout d'abord été relevé l'exploitation d'un outil de messagerie qui n'avait pas fait l'objet par le responsable de traitement de la formalité préalable requise à sa mise en œuvre.

De plus, il a été constaté l'absence d'une politique/procédure uniformisée sur le sort des boîtes email nominatives applicable en cas de départ définitif de salariés, ce qui est contraire aux dispositions de l'article 10-1 de la Loi n° 1.165 et ne correspond pas aux recommandations sur les traitements automatisés de données personnelles dans le cadre de la gestion de la messagerie professionnelle définies au sein de la délibération n° 2015-111. En effet, il a été relevé une absence de blocage systématique des adresses email au départ définitif du salarié et une absence de suppression systématique de la boîte nominative dans les 3 mois maximum suivant son départ.

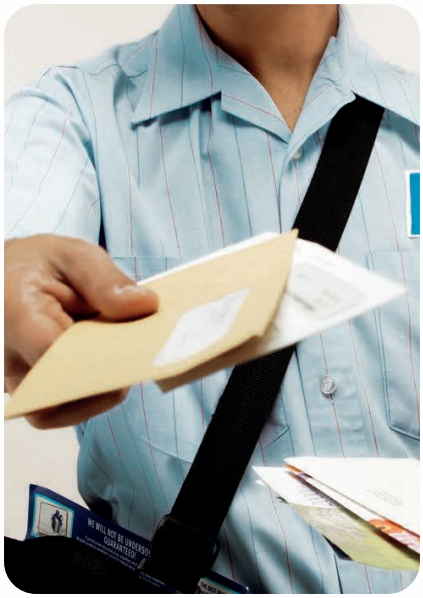
Il a également été constaté qu'au départ définitif de certains salariés des délégations d'accès étaient accordées sur leurs messageries nominatives à d'autres collaborateurs encore en poste et ce plus de 3 mois après le départ définitif des premiers, ce qui est susceptible de constituer une atteinte à la vie privée des personnes concernées.

Par ailleurs, il a été relevé la conservation automatique de la copie de l'ensemble des emails de la société pouvant conduire à un contrôle permanent et continu des salariés et porter atteinte à leur vie privée.

S'agissant de l'information des salariés sur ce traitement il a été constaté que la charte informatique qui leur avait été communiquée était lacunaire, notamment sur les comportements attendus des salariés dans l'utilisation de l'outil mis à leur disposition et plus particulièrement sur les moyens d'identification des messages privés échangés depuis la messagerie professionnelle.

Il a en outre été relevé des non conformités à l'article 17 de la Loi n° 1.165 relatif aux mesures techniques à mettre en œuvre pour garantir la sécurité et l'intégrité des informations nominatives traitées notamment concernant la politique de renouvellement des mots de passe ainsi que sur la maîtrise des personnes ayant accès au traitement.

Le rapport relevant les irrégularités constatées lors des opérations d'investigation a été notifié au responsable des locaux en septembre 2025 afin qu'il puisse y répondre dans un délai d'un mois. L'APDP se prononcera sur les suites à donner à ces irrégularités à l'issue de ce délai.



Investigation relative à l'utilisation et à l'envoi de données personnelles

La CCIN a mené une investigation portant sur l'élaboration d'un document dont l'existence avait été révélée par la presse, afin de vérifier si les éléments mentionnés à l'encontre du plaignant étaient corrélés par un traitement d'informations nominatives qu'il estimait nécessairement illicite, les informations connues de celui-ci relativement à sa carrière n'étant pas de nature à contenir les informations publiques incriminées. A l'issue des opérations de contrôle, la CCIN n'a trouvé ni traitement illicite, ni informations négatives relatives au plaignant permettant de corroborer les allégations publiques. Elle n'a ainsi pas trouvé l'auteur du document, ni ses destinataires.

Les mesures correctrices et les sanctions

En 2024, le Président de la CCIN a prononcé à l'encontre d'un restaurant une mise en demeure non publique de procéder à la régularisation du système de vidéosurveillance ou au retrait de l'ensemble des caméras dans un délai de 30 jours maximum.

Cette sanction est intervenue suite à une investigation sur place qui a donné lieu à la rédaction d'un rapport listant les manquements relevés et transmis au responsable des locaux qui n'a adressé aucune observation en retour.

Lors des opérations de contrôle, il avait été constaté une exploitation illicite d'un dispositif de vidéosurveillance composé de plusieurs caméras orientables manuellement et dotées de détecteurs de mouvement dont une permettait de filmer de manière incidente la voie publique.

De plus, le système était géré depuis une application mobile installée sur le téléphone du gérant de l'établissement permettant un possible accès en continu aux images et susceptible d'engendrer un risque important d'atteinte à la vie privée des clients et des salariés.

Par ailleurs, aucun affichage ne permettait d'informer les personnes concernées sur l'existence d'un système de vidéosurveillance contrairement à l'article 14 de la Loi n° 1.165 et de la recommandation n° 2010-13 de la CCIN portant recommandation sur les dispositifs de vidéosurveillance mis en œuvre par des personnes physiques ou morales de droit privé.

Une seconde mise en demeure a concerné un autre restaurant, et a fait suite à un contrôle réalisé en 2023, au cours duquel il avait été constaté que certaines caméras exploitées n'étaient pas couvertes par le périmètre de l'autorisation délivrée par la CCIN, et que d'autres caméras permettaient de filmer l'intérieur d'un commerce voisin.

Suite à cette mise en demeure la situation a été régularisée.

Faisant suite à un contrôle effectué en 2023, un commerce a fait l'objet d'un avertissement début 2024. Les opérations de contrôle avaient mis en lumière l'exploitation illicite de caméras de vidéosurveillance, lesquelles permettaient en outre de surveiller les salariés, et surtout d'écouter en temps réel les conversations au sein de cet établissement.

Suite à cette sanction le dispositif a été désactivé sur le champ.

L'exercice du droit d'accès indirect

En 2024 la CCIN a été saisie d'une demande de droit d'accès indirect, relativement à des informations traitées par la Direction de la Sûreté Publique relatives au plaignant qui avait su qu'il était défavorablement connu des Services de Police.

Afin de vérifier les informations détenues sur lui le Magistrat du siège accompagné d'un Agent assermenté se sont rendus dans les locaux de la DSP, le Président a saisi de cette question le Ministre d'Etat.

En fin d'année 2024 ce dossier n'avait donné lieu à aucune réponse, et son examen se poursuivra en 2025.

4

LES AVIS SUR LES PROJETS DE TEXTES

Projets de modification de l'Ordonnance Souveraine n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé et de modification de l'Arrêté Ministériel n° 2020-764 du 5 novembre 2020 portant application de l'Ordonnance Souveraine relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé.

Le 30 janvier 2024, le Ministre d'Etat a saisi la CCIN d'un projet de modification de l'Ordonnance Souveraine n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé ainsi que d'un projet de modification de l'Arrêté Ministériel n° 2020-764 du 5 novembre 2020 portant application de l'Ordonnance Souveraine relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé ; textes pour lesquels elle avait déjà rendu des avis dans 3 délibérations en date du 18 septembre 2019 (délibération n° 2019-122) et du 17 juin 2020 (délibérations n° 2020-103 et 2020-104).

Dans sa délibération n° 2024-105 du 15 mai 2024 portant avis sur ces projets, la Commission a pris acte que les deux projets de texte qui lui ont été soumis avaient pour objectif de supprimer toute référence au référentiel d'exigences concernant la qualification des

Prestataires d'Informatique en Nuage et d'Hébergement (PINH) s'agissant des hébergeurs de données de santé, et s'est toutefois inquiétée du possible impact que la révision du référentiel HDS allait avoir sur les deux textes révisés.

Le Ministre d'Etat avait en effet souligné dans son courrier de saisine que ce référentiel n'existant pas en France, il « *a pour conséquence de décourager l'installation et le développement de prestataire HDS [Hébergeur de Données de Santé] en Principauté* ».

A cet effet, l'article 5 de l'Arrêté Ministériel n° 2020-764 du 5 novembre 2020 qui traite de la qualification d'hébergeur de données de santé prévoit le respect de deux référentiels, dont le référentiel PINH, ainsi que le référentiel HDS français.

La Commission a néanmoins tenu à souligner que le référentiel HDS qui permet de garantir la sécurité de l'hébergement des données de santé, en certifiant les hébergeurs qui mettent en œuvre des systèmes de gestion de la sécurité des systèmes d'information à l'état de l'art des normes internationales, avait été récemment modifié et que suite à l'avis favorable de la Commission nationale de l'informatique et des libertés (CNIL) le 13 juillet 2023, une version révisée devait entrer en vigueur au cours de l'année 2024.

Or, ladite version a ajouté notamment quatre exigences relatives à la souveraineté des données, devant faire l'objet d'une mise à jour de la part des entreprises déjà certifiées.

Celles-ci sont les suivantes :

« ***Exigence 28 : Localisation des données de santé*** – *Désormais, les données de santé doivent être physiquement hébergées uniquement dans un pays membre de l'Espace Économique Européen (EEE), incluant l'Union Européenne (UE), la Norvège, l'Islande, et le Liechtenstein.*

Exigences 29 et 30 : Accès distant et législation extra-européenne – *Si l'accès aux données se fait depuis un pays hors UE, que ce soit par l'hébergeur ou un sous-traitant, ou si ces derniers sont soumis à une législation extra-européenne ne fournissant pas un niveau de protection adéquat selon l'article 45 du RGPD, l'hébergeur doit en informer ses clients dans le contrat. Il doit également préciser les risques associés et les mesures techniques et juridiques prises pour les limiter.*

Exigence 31 : Publication des transferts de données – *Les hébergeurs doivent publier sur leur site internet une cartographie des transferts de données vers des pays hors de l'EEE.* »

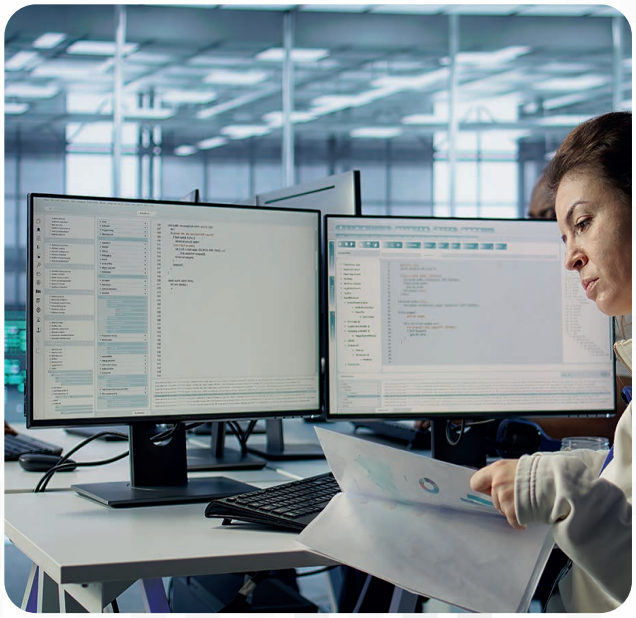
Sur ce point, la Commission a relevé que le projet de modification de l'article 5 de l'Arrêté Ministériel n° 2020-764 maintenait la nécessité pour un hébergeur de données de santé d'obtenir la certification qu'il respecte le référentiel HDS français pour pouvoir obtenir la qualification HDS de la part du Directeur de l'AMSN.

A cet égard elle a souligné que l'introduction des nouvelles exigences liées à la souveraineté des données au sein du référentiel HDS français (et plus particulièrement de l'Exigence n° 28) pouvait être de nature à entraver la délivrance de la qualification HDS pour des hébergeurs de données de santé ayant une activité en lien avec la Principauté.

De ce fait la Commission a invité à une modulation de la rédaction de l'article 5 en projet afin de tenir compte de la révision du référentiel HDS, qui devait être appliquée courant de l'année 2024.

Projets d'Ordonnances Souveraines portant sur la mise à disposition de l'Etat des données relatives à la distribution et à la fourniture de gaz, d'électricité, de chaud et de froid et relatives à la mise à disposition des données de comptage d'énergie aux propriétaires ou syndicats de copropriétaires des immeubles bâtis et projet d'Arrêté Ministériel déterminant les données relatives à la distribution et à la fourniture de gaz, d'électricité, de chaud et de froid mises à disposition de l'Etat et fixant les modalités de cette mise à disposition

Le Ministre d'Etat a saisi la Commission de trois projets de textes qui s'inscrivent dans la lignée des textes français destinés à favoriser la transition énergétique et réduire les émissions de gaz à effet de serre, telle que la Loi n° 2015-992 du 17 août 2015 relative à la transition énergétique pour la croissance verte, et ses Décrets d'application. La CCIN a rendu son avis sur ces projets par délibération n° 2024-135 du 12 juin 2024.



A titre liminaire, la Commission a constaté que ces textes viennent s'ajouter au corpus de textes déjà existants dans le domaine et a ainsi regretté que l'encadrement de l'énergie soit in fine éclaté sur plusieurs textes qui ne feront pas l'objet d'une consolidation/codification. A titre d'exemple, les modalités d'exploitation de la courbe de charge seraient donc réparties sur quatre textes distincts, sans texte « *chapeau* », ce qui dilue les objectifs des dispositions adoptées (ou les rend redondantes) et donc les finalités potentielles d'exploitation des données personnelles.

Enfin, la Commission a relevé que le jumeau numérique de la Principauté permet la mise à disposition des consommations énergétiques des bâtiments, ce qui n'est pas prévu par les dispositions projetées. La Commission s'est donc interrogée sur la licéité de cette mise à disposition à l'aune des textes projetés.

Sur le projet d'Ordonnance Souveraine relative à la mise à disposition de l'Etat des données relatives à la distribution et à la fourniture de gaz, d'électricité, de chaud et de froid

La Commission a estimé que le texte projeté rend difficile la compréhension des flux de données que le Gouvernement entend mettre en place, les destinataires des informations au sein de l'Etat n'étant pas définis et les missions pour lesquelles les données sont communiquées pas clairement identifiées.

Elle a relevé qu'aucun régime de sanction n'est prévu en cas de communication ou d'utilisation indue de données protégées, seul étant mentionné, au sein de l'Arrêté Ministériel d'application de l'Ordonnance projetée, le secret professionnel de l'article 308 du Code pénal auquel sont soumis les agents qui reçoivent communication des données.

La Commission a ensuite constaté qu'aux termes « *à partir des données issues de son système de comp-*

tage d'énergie » de l'article français dont le texte monégasque s'inspire, se substitue dans le projet les termes « à partir de leur système de comptage ». Le choix textuel monégasque semble ainsi laisser entendre que l'Etat pourrait, pour la mise à disposition de données, solliciter un accès direct aux systèmes métiers des Concessionnaires. Un tel choix n'étant ni proportionné, ni de nature à restreindre les communications de données comme cela est prévu dans d'autres articles du projet d'Ordonnance, la Commission a recommandé de reprendre la terminologie française.

Par ailleurs, la Commission n'a pas été en mesure de comprendre l'objectif de l'article 3 projeté qui liste les informations commercialement sensibles dont les Concessionnaires sont tenus d'assurer la confidentialité, et dont la teneur est modifiée par rapport au texte français dont il s'inspire. Il s'applique en effet à tout « *client final* » quand le texte français s'applique aux « *dispositions des contrats et protocoles d'accès aux réseaux publics de transport ou de distribution mentionnés aux articles L. 111-91 et L. 111-92* » qui ne sont pas des clients personnes physiques.

A la lecture de l'article 4 projeté qui prévoit l'inopposabilité du secret des informations commercialement sensibles aux fonctionnaires et agents habilités de l'Etat agissant dans le cadre de leur mission de suivi et de contrôle, la Commission a relevé que cette disposition fait peser de graves problèmes de respect de la vie privée des personnes concernées, le texte en projet semblant permettre la communication des contrats et des courbes de charges individuelles de personnes physiques.

La Commission a relevé que l'article 4 projeté avait pour but de permettre un contrôle des Concessionnaires par la Direction de l'Aménagement Urbain, cette dernière étant chargée « *de contrôler l'application des cahiers des charges des concessions de service public de la distribution d'énergie électrique et de gaz naturel, de production et de distribution de chaleur et de froid, de distribution d'eau potable et d'exploitation de l'usine de traitement des eaux résiduaires, de nettoiement des voies publiques, de collecte et d'incinération des résidus urbains* ». Elle a toutefois estimé que si tel était le cas, l'introduction de l'article 4 participait à la confusion quant aux objectifs du projet d'Ordonnance, entre l'unique objectif affiché du respect des normes environnementales et de préservation de l'énergie, auquel s'ajouteraient l'encadrement du fonctionnement des concessions et d'éventuels pouvoirs d'enquête.

Sur le projet d'Arrêté Ministériel déterminant les données relatives à la distribution et à la fourniture de gaz, d'électricité, de chaud et de froid mises à disposition de l'Etat et fixant les modalités de cette mise à disposition

Ce projet d'Arrêté listait les informations communiquées à l'Etat et les conditions de cette communication en application du projet d'Ordonnance Souveraine susvisé.

La Commission s'est étonnée que le texte prévoyait une communication horaire de données, et s'est interrogée sur la pertinence d'une telle précision dans le pilotage de la politique énergétique de la Principauté, d'autant que cela pourrait s'avérer problématique quand un bâtiment appartient à un propriétaire unique ou une industrie.

La Commission s'est également interrogée sur le fait que les dispositions projetées indiquaient qu'un réseau de chaud et de froid est constitué par « *deux usagers* » alors qu'aucune donnée ne peut être transmise en application de l'article 3 de l'Arrêté projeté en dessous du seuil d'« *au moins 10 points de livraison actifs* » quand des personnes physiques sont concernées.

Elle a relevé en outre que ne sont pas protégées les données dont les titulaires de contrats ne sont pas des personnes physiques. La Commission a estimé que ce choix permettait la transmission de données résidentielles de personnes physiques disposant d'un logement de fonction, ou de personnes physiques domiciliées dans leur lieu d'exercice et qui auraient contracté sous le nom de leur structure. Elle a de ce fait recommandé de modifier ce choix rédactionnel afin de prendre en compte la destination du point de livraison.

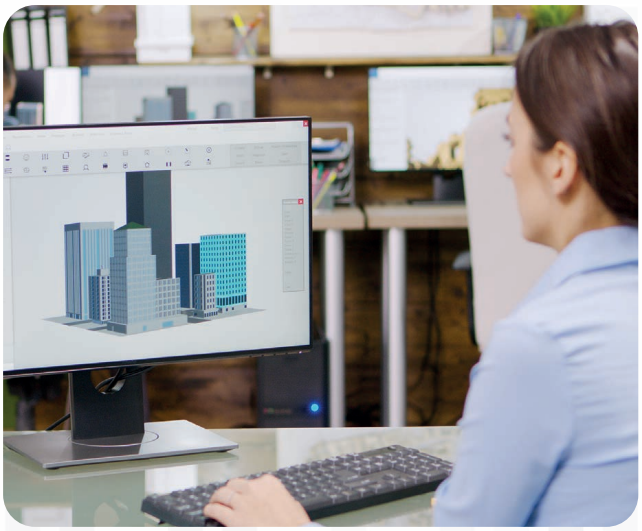
L'article 4 projeté faisait également état d'un « *cadastre énergétique de la Principauté* » à établir sans que ce document ne soit défini. Il résulte des informations accessibles en ligne par les acteurs de l'énergie qu'un cadastre énergétique est un outil de gestion qui permet de classer différents immeubles en fonction de leur qualité énergétique et donc de l'urgence d'entreprendre des rénovations, il fait apparaître le(s) bâtiment(s) qui présente(nt) le plus gros potentiel d'économies d'énergie, et porte uniquement sur le poste chauffage.

La Commission a estimé qu'à défaut de toute information, notamment la qualité exacte des données de consommation nécessaires à l'établissement du cadastre, il ne lui était pas possible de se prononcer sur la proportionnalité et l'adéquation des informations nominatives recueillies par bâtiment, notamment dans le cas où seul un abonné y résiderait, générant ainsi un risque d'atteinte au droit au respect à la vie privée et familiale. En l'absence d'une politique définie de

rénovation énergétique, la Commission s'est interrogée sur la balance risque/bénéfice d'une telle mesure : la Direction de l'Environnement, en analysant qu'un immeuble surconsomme, peut-elle inciter les propriétaires à des travaux de rénovation énergétique ?

S'il était mentionné que les données seront anonymisées à l'issue de l'établissement du cadastre énergétique, la Commission s'est interrogée sur ce que cela signifiait concrètement, dans la mesure où les rapports des consommations et l'immeuble concerné seront nécessairement conservés pour établir le plan d'intervention et pouvoir in fine comparer le gain opéré.

L'article 5 prévoyait quant à lui que les mises à disposition de données s'effectuent par le biais d'une plateforme. Toutefois, la rédaction monégasque projetée ne permettait pas de savoir s'il s'agissait de la plateforme gérée par le Concessionnaire ou l'Autorité concédante. En outre, les précisions sur l'utilisation d'API interpellaient la Commission. La volonté est-elle de mettre en place une automatisation des communications directement issues de collectes effectuées par les Concessionnaires, notamment pour les données transmissibles au titre de l'article 3 de l'Arrêté Ministériel projeté ? La Commission a recommandé de supprimer cet élément.



Sur le projet d'Ordonnance Souveraine relative à la mise à disposition de données de comptage d'énergie aux propriétaires ou syndicats de copropriétaires des immeubles bâtis

Ce projet d'Ordonnance visait à mettre à disposition les données de consommation des occupants, aux propriétaires ou syndicats de copropriétaires d'immeubles bâtis en faisant la demande, comptant plus de dix abonnés et qui justifient d'actions de maîtrise de la consommation en énergie de leurs occupants. Il était grandement inspiré, au sein de la partie réglementaire du Code de l'énergie français, de la Section 4 « *Mise à disposition des données de comptage de consommation aux propriétaires ou gestionnaires d'immeubles (Articles D341-13 à D341-17)* » du Livre III Titre IV Chapitre I[er].

La Commission a uniquement recommandé d'ajouter un article identique à l'article D 341-17, lequel dispose qu'« *Il est interdit au propriétaire ou au gestionnaire de l'immeuble, sauf autorisation expresse de chaque occupant, de chercher à reconstituer les données individuelles de comptage* ».

5

LES DÉLIBÉRATIONS PORTANT RECOMMANDATION

La CCIN a été saisie de plusieurs plaintes émanant d'anciens fonctionnaires qui avaient fait l'objet de mesures disciplinaires ayant conduit à leur révocation, plusieurs années auparavant. Toutefois la non désindexation des Ordonnances Souveraines publiées au Journal de Monaco conduisait à entraver leur réinsertion professionnelle.

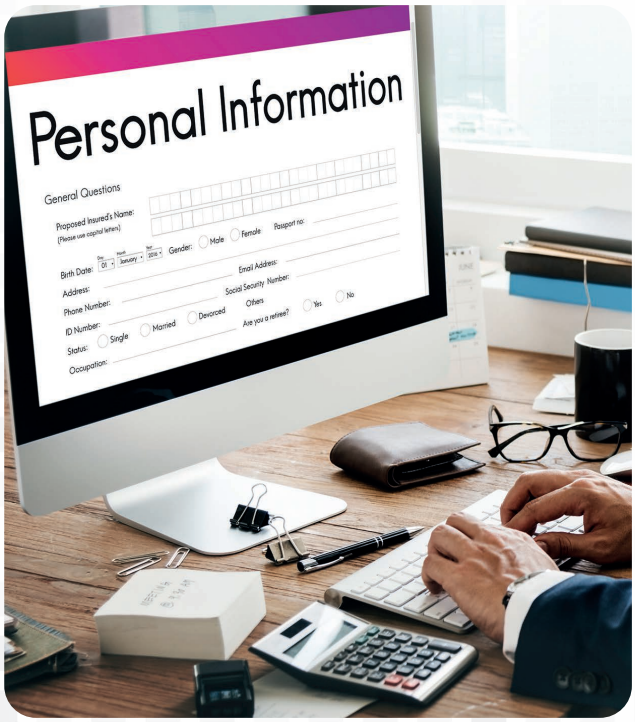
Les échanges avec les Services concernés n'ayant pas abouti, la CCIN a décidé de formuler une recommandation sur ce point.

A cette occasion elle a également formulé une recommandation afin que les Ordonnances Souveraines prononçant une mise en inactivité pour invalidité ne mentionnent désormais plus ce motif, afin que la vie privée des personnes concernées soit respectée.

Délibération n° 2024-071 du 20 mars 2024 portant recommandation sur la publication au Journal de Monaco des Ordonnances Souveraines et des Arrêtes Municipaux de mise à la retraite pour invalidité.

La CCIN a constaté que lorsque des fonctionnaires de l'Etat ou de la Commune font l'objet d'une mise à la retraite pour invalidité, l'Ordonnance Souveraine ou l'Arrêté Municipal la prononçant mentionne ce motif de mise à la retraite. Ces mesures font l'objet d'une publication au Journal de Monaco. Dès lors, les tiers sont avisés de ce que l'état de santé des personnes concernées impose leur mise à la retraite pour invalidité, ce qui revient à divulguer leurs données de santé et peut nuire au droit au respect de leur vie privée.

Cette question revêt une acuité particulière du fait de la diffusion au format numérique du Journal de Monaco, qui a pour conséquence que ces publications demeurent accessibles sans limitation de durée, à toute personne faisant une recherche Internet à partir du nom des fonctionnaires concernés.



La CCIN a considéré que l'indication de ce motif dans un acte rendu public et soumis à une large diffusion ne peut être justifiée par aucun motif valable de nature supérieure à l'intérêt pour les personnes objets de la mesure à voir respecter leur droit à la vie privée, en effet :

- les tiers n'ont aucun intérêt objectif à connaître le motif de la mise à la retraite dès lors qu'il résulte d'un constat médical faisant grief uniquement à la personne concernée ;
- aucune des dérogations à l'utilisation de données sensibles prévues à l'article 12 de la Loi n° 1.165 n'a vocation à s'appliquer, le motif d'intérêt public ne justifiant pas la publication de données de santé, pas plus que les articles 54 bis de la Loi n° 975 portant statut des fonctionnaires de l'Etat et 50-1 de la Loi n° 1.096 portant statut des fonctionnaires de la Commune n'imposent de le faire ;
- le fait que la décision de mise à la retraite pour invalidité peut être contestée par la personne concernée n'est pas plus de nature à justifier l'indication du motif d'ordre médical dans l'Ordonnance Souveraine ou l'Arrêté Municipal y afférent. La décision de mise à la retraite pour invalidité intervient en effet à l'issue d'un processus contradictoire basé sur l'état de santé du fonctionnaire et peut lui être notifiée par tout moyen, autre qu'une publication, ayant date certaine et pouvant faire l'objet d'un recours de sa part.

Aussi, compte tenu des différents intérêts en balance, et au nécessaire respect dû à la vie privée des fonctionnaires concernés, la Commission a estimé que les Ordonnances Souveraines et les Arrêtés Municipaux portant mise à la retraite pour invalidité ne devraient plus à l'avenir comporter le motif de la mise à la retraite de la personne concernée mais se limiter à mentionner que le fonctionnaire est admis à faire valoir ses droits à la retraite.

Depuis, le Gouvernement ne mentionne plus ce motif dans ses décisions publiées au Journal Officiel.

Délibération n° 2024-072 du 20 mars 2024 portant recommandation sur l'évolution des dispositions conduisant à publier automatiquement certaines sanctions disciplinaires des personnels du Secteur Public au Journal de Monaco et la mise en œuvre d'un droit à l'oubli.

La CCIN a été saisie de plusieurs plaintes émanant d'anciens fonctionnaires de l'Etat ayant été révoqués par Ordonnance Souveraine. Ces derniers s'estiment préjudiciés dans leur vie privée et familiale car ils apparaissent toujours, plusieurs années après, dans les recherches effectuées sur Internet à partir de leurs noms, que ce soit à partir du site Internet du Journal de Monaco, ou des moteurs de recherches généralistes. Ils se trouvent ainsi préjudiciés de manière imprescriptible dans leurs recherches d'emploi.

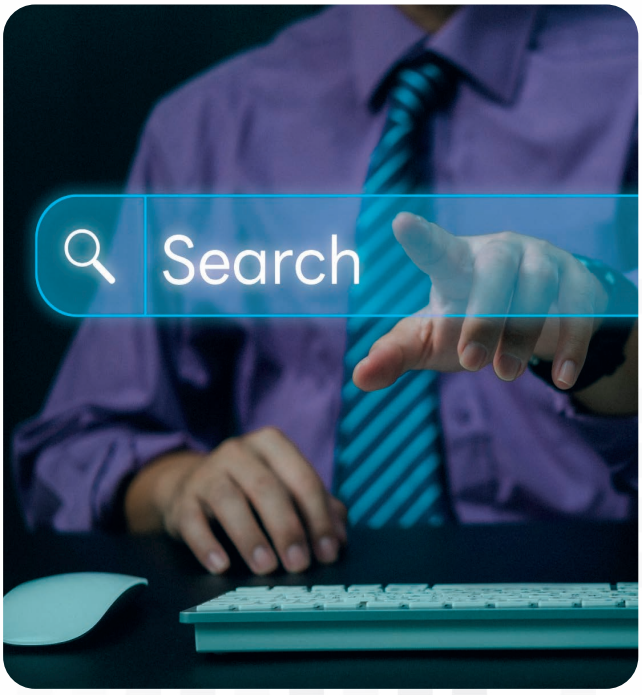
Après étude, la Commission a pu relever que la problématique soulevée en Principauté s'étendait au-delà des seuls cas des personnes ayant saisi la CCIN, mais concerne de manière générale tous les personnels d'entités publiques ou relevant de régimes spéciaux dont les sanctions sont automatiquement publiées au Journal Officiel de Monaco, et donc publiées sur le site Internet de ce dernier. A partir de ce site, d'autres moteurs de recherche extraient ces informations pour les référencer sur leurs propres sites, relayant ainsi l'information.

La CCIN a souhaité prendre une recommandation pour aborder cette problématique sous trois de ses aspects, ce qui a conduit à une prise en compte de la problématique par le Gouvernement.

Sur l'automaticité de la publication des sanctions

A partir d'un certain degré de gravité de la faute commise, la sanction de certains personnels du Secteur public fait l'objet d'une publication automatique. Or, cette publication constitue une ingérence dans le droit à la vie privée et familiale de la personne concernée en ce qu'elle rend publique la sanction disciplinaire prononcée à son encontre.

La Commission estime donc, comme c'est le cas dans la législation en matière de protection des données, et comme c'est le cas pour les autres Autorités Administratives Indépendantes, que la publicité doit s'analyser comme une mesure autonome au sein d'une sanction, et qui ne devrait pas être automatique. Il a toutefois été indiqué à la CCIN que c'est l'application de l'article 1er alinéa 2 de la Loi n° 884 du 29 mai 1970 sur l'entrée en vigueur et l'opposabilité des Ordonnances Souveraines et Arrêtés Ministériels et autres décisions administratives qui obligerait à procéder ainsi afin de rendre la décision opposable à la personne concernée et aux tiers.



La CCIN a néanmoins rappelé que :

- c'est la décision de sanction qui lui fait grief, et non la publication au Journal Officiel ;
- concernant les tiers, si l'objectif est que le public puisse avoir connaissance qu'une personne n'appartient plus à l'Administration afin qu'elle ne puisse plus se prévaloir des prérogatives de ses anciennes fonctions, il n'est pas intrinsèquement lié à l'information d'une sanction, ni même, dans l'absolu, à la nécessité d'une publication par Ordonnance Souveraine, si d'autres moyens existent pour informer les administrés.

Sur l'indexation automatique des sanctions

En ce qui concerne les sanctions dont il aura été fait le choix de la publication, la Commission estime qu'il conviendra de ne plus les rendre indexables par les moteurs de recherche et donc, comme l'indique le rapporteur public du Conseil d'Etat français concernant l'affaire Théâtre National de Bretagne (n° 389448) du 28 septembre 2016, de recréer en ligne les conditions de consultation d'un journal officiel papier. Le Journal de Monaco numérique ne contiendrait ainsi la sanction qu'au sein de la version PDF et ne se retrouverait pas dans la partie indexée consultable en ligne.

Sur l'application du droit à l'oubli

En l'absence des mesures précédemment évoquées, se pose nécessairement la question du droit à l'oubli.

Si la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives ne prévoyait pas expressément de droit à l'oubli, la jurisprudence de la Cour Européenne des Droits de l'Homme chargée de veiller à l'application de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, à laquelle la Principauté de Monaco est Partie, le reconnaît expressément.

Pour apprécier si ce droit à l'oubli destiné à protéger le droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention européenne, susvisée, qui inclut le droit à la protection de la réputation, doit s'appliquer, la Cour européenne met en balance notamment la nature de l'information archivée, le temps écoulé depuis les faits, la première publication et mise en ligne, l'intérêt contemporain pour l'information contenue dans la publication, l'intérêt du public à accéder à cette information, la notoriété de la personne et les répercussions négatives de la mise en ligne sur la personne concernée ainsi que l'impact de la mesure d'oubli. Ce droit à l'oubli s'applique aux condamnations pénales et doit trouver à s'appliquer aux sanctions disciplinaires.

Il convient ainsi d'apprécier si le maintien du référencement (indexation) de ces sanctions disciplinaires reste justifié sans limitation de durée. Le fait de maintenir référencées / indexées sur le site Internet du Journal de Monaco de telles Ordonnances Souveraines sans limitation de durée ne peut être considéré par la CCIN comme étant nécessaire à l'information du public.

Ce maintien fait perdurer les effets négatifs de la publication initiale sans limite temporelle. Il fait également bien souvent obstacle à une recherche d'emploi de la personne concernée et ainsi porter atteinte à sa réputation sans tenir compte de son comportement actuel.

Une réponse légale (partielle) à la problématique

Un début de réponse à la problématique soulevée a été introduit à l'article 13 Loi n° 1.578 du 1er juillet 2025 portant modification de diverses dispositions en matière de numérique qui modifie la Loi n° 1.383 du 2 août 2011 et insère un article 53-1 qui dispose que « *Certains actes individuels, notamment relatifs à l'état et à la nationalité des personnes, doivent être publiés dans des conditions garantissant qu'ils ne font pas l'objet d'une indexation par des moteurs de recherche.*

Les catégories d'actes individuels mentionnées au premier alinéa qui ne peuvent être publiés par Ordonnance Souveraine que dans des conditions garantissant qu'ils ne font pas l'objet d'une indexation par des moteurs de recherche, sont déterminées par Ordonnance Souveraine. »

Par ailleurs le Ministre d'Etat a indiqué à la CCIN qu'une réflexion sur ce point allait être entreprise. Toutefois, à ce jour, aucune modification de ces pratiques n'est intervenue.

6

LES TRAITEMENTS AUTOMATISÉS D'INFORMATIONS NOMINATIVES

Le répertoire public des traitements

En application de la Loi n° 1.165, 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.

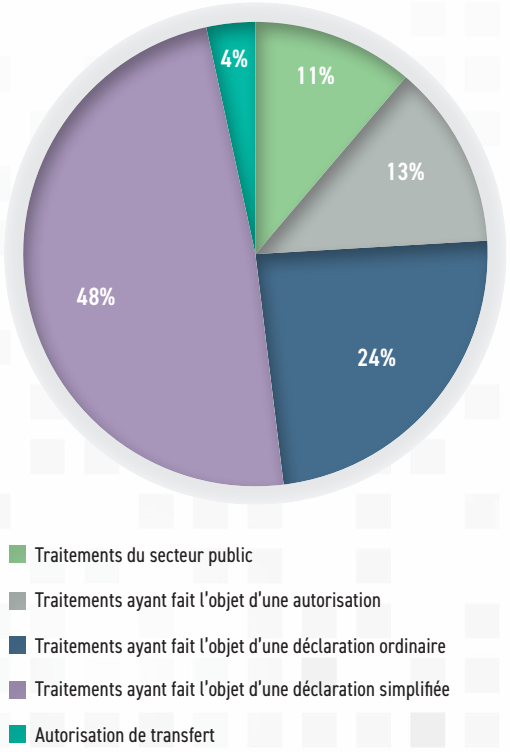
Il peut être consulté au siège de la Commission par toute personne physique ou morale souhaitant s'assurer de l'existence légale d'un traitement automatisé d'informations nominatives.

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 2024 :

7.916 *se répartissant ainsi :*

- ***898*** traitements du secteur public ou assimilé ;
- ***1.035*** traitements ayant fait l'objet d'une autorisation de la Commission ;
- ***1.902*** traitements ayant fait l'objet d'une déclaration ordinaire ;
- ***3.795*** traitements ayant fait l'objet d'une déclaration simplifiée ;
- ***286*** autorisations de transfert vers un Pays ne disposant pas d'un niveau de protection adéquat.



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	2024
DS								46	19	54	856	144	86	180	201	162	221	243	328	188	117	206	227	87	170
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	111
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	61
DAUT												38	38	31	87	62	89	119	90	97	72	91	64	74	74
TRANSFERT														1	1	4	21	21	41	29	26	54	32	24	32

Nombre de nouveaux traitements inscrits au répertoire en 2024 :

448 traitements ont été inscrits en 2024 au répertoire public, se répartissant comme suit :

61 traitements ayant fait l'objet d'un avis favorable à leur mise en œuvre, relevant du secteur public ou assimilé ;

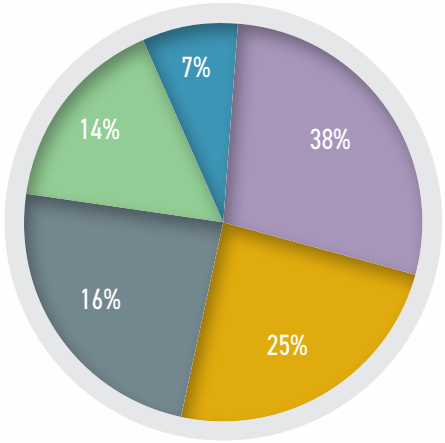
74 traitements dont la mise en œuvre a été autorisée par la Commission ;

111 traitements ayant fait l'objet d'une déclaration ordinaire ;

170 traitements ayant fait l'objet d'une déclaration simplifiée ;

32 autorisations de transfert de données vers un Pays ne disposant pas d'un niveau de protection adéquat.

RÉPARTITION DES NOUVEAUX TRAITEMENTS INSCRITS EN 2024



- 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

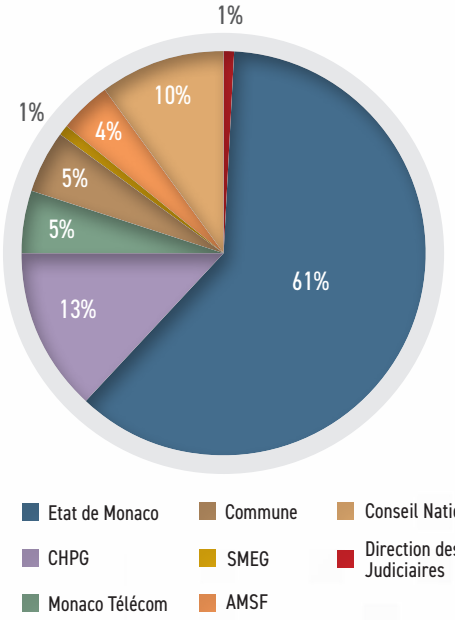
Nombre de délibérations rendues par la Commission en 2024 :

Au cours de l'année écoulée, la Commission a rendu ***217*** délibérations se répartissant comme suit :

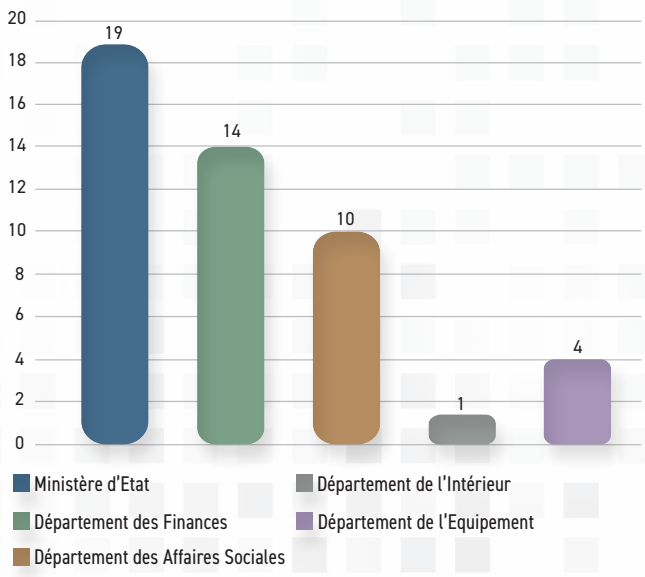
- ***91*** autorisant la mise en œuvre ou la modification de traitements
- ***79*** portant avis favorable à la mise en œuvre ou à la modification de traitements
- ***32*** autorisant un transfert d'informations nominatives vers un Pays ne disposant pas d'un niveau de protection adéquat
- ***2*** portant avis sur des projets de textes transmis par le Ministre d'Etat
- ***9*** portant sur une mission d'investigation
- ***1*** portant refus d'autorisation
- ***1*** portant avis défavorable
- ***2*** portant recommandation

Les traitements du secteur public

Avis favorables rendus en 2024



Les Départements de l'Etat concernés



La moitié des avis favorables rendus par la Commission en 2024 ont concerné des traitements soumis par les Services de l'Etat.

Depuis l'entrée en vigueur de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles, qui a abrogé la Loi n° 1.165 du 23 décembre 1993, très peu de traitements sont désormais soumis à formalité préalable auprès de l'APDP.

Filtrage des accès internet des élèves DENJS

La Direction de l'Education Nationale de la Jeunesse et des Sports (DENJS) a soumis à l'avis de la Commission un traitement ayant pour finalité « *Gestion de la politique de filtrage des accès à Internet des établissements scolaires* ». L'objectif de celui-ci est la sécurisation des accès à Internet des personnes que la DENJS a dotées d'un poste de travail numérique.

Ce traitement prévoit le filtrage de tout trafic reçu d'un utilisateur (http et https), connecté au réseau interne de la DENJS, ou à un réseau externe, par rapport à des règles prédéfinies et appliquées selon le profil de l'utilisateur (lycéen, collégien, enseignant). Dans l'hypothèse où une recherche Internet enfreint une de ces règles, elle est bloquée.

Par ailleurs, en plus du blocage de la recherche, la DENJS avait sollicité l'avis de la Commission sur la génération automatique d'alertes, dès la première recherche bloquée. Ainsi, la DENJS souhaitait qu'une alerte automatique soit générée à chaque recherche bloquée en indiquant que celle-ci serait ensuite analysée par son Service informatique afin d'écarter les faux positifs. De plus, la DENJS a précisé qu'en cas d'alerte avérée, il serait procédé à la notification de la personne concernée ou encore à sa convocation, et en fonction de la gravité et de la récurrence, à l'information des Conseillers Principaux d'Education et des fonctions de Direction.

La DENJS justifiait la génération automatique d'alertes en indiquant que cette mesure était nécessaire pour la protection des mineurs.

Considérant que l'objectif de protection des mineurs « *est dans la plus grande majorité des cas atteint dès lors que la recherche intentée par l'élève est bloquée, et ainsi, que le déclenchement automatique d'une réponse individuelle et nominative est disproportionné avec le but recherché* », la Commission a demandé au responsable de traitement de procéder à la suspension des alertes et des contrôles individuels tels que prévus.

Toutefois, la Commission a demandé au responsable de traitement de revenir vers elle avec une demande

d'avis modificative, s'il estimait toujours nécessaire d'introduire cette fonctionnalité, en « *explicitant notamment la procédure permettant de déterminer les mécanismes mis en œuvre pour respecter à la fois la sécurité du système d'information, la prévention d'infractions [...], et le respect de la vie privée des personnes concernées. Cette proportionnalité pourrait trouver sa source dans la mise en œuvre d'une pseudonymisation des alertes, d'établissement de scénarii permettant d'effectuer des réponses graduées aux problèmes rencontrés, l'éventuelle implication d'une équipe pédagogique pour déterminer les suites à donner à une alerte* ».

Enfin, la Commission a attiré l'attention du responsable de traitement sur la qualité de l'information dispensée aux personnes concernées ainsi que sur la prise en considération du destinataire de l'information avec par exemple la communication d'un document adapté aux élèves.

L'emplacement des caméras dans les écoles et crèches

Courant 2024, la Commission a été saisie de plusieurs demandes d'avis concernant des dispositifs de vidéosurveillance installés dans des écoles et des crèches afin d'**assurer la sécurité des biens et des personnes.**

Si elle comprend cet intérêt, la Commission est néanmoins extrêmement vigilante au respect des **droits et libertés des personnes concernées**, et en particulier

des **enfants** et du **personnel**, en vérifiant notamment que l'implantation de tels dispositifs n'empiète pas sur la sphère privée desdites personnes.

Elle tient donc à rappeler les règles suivantes concernant l'emplacement des caméras dans les écoles et crèches :

Ce qui est autorisé

- les entrées et sorties, les issues de secours, en faisant attention à ne pas filmer les bâtiments avoisinants ;
- les **principaux** espaces de circulation ;
- les portes des ascenseurs ;
- les casiers en cas d'actes de malveillance fréquents et répétés.

Ce qui est interdit

- les cours de récréation, les préaux, les espaces de jeu, les salles de sport, les lieux de restauration ;
- les salles de classe ;
- l'intérieur des ascenseurs ;
- la ou les salle(s) de réunion ;
- les bureaux ou poste de travail du personnel ;
- les lieux mis à la disposition des salariés à des fins de détente ou de pause déjeuner (salle de repos, kitchenette, canapés, espace fumeur, etc.) ;
- les accès, fenêtres, cour(s) et/ou terrasses des immeubles voisins.

La plateforme pour l'emploi

La Direction du Travail a sollicité l'avis de la CCIN préalablement à la mise en œuvre d'une nouvelle plateforme pour la gestion de l'emploi en Principauté dont l'objectif est de permettre la création d'espaces personnalisés pour les demandeurs d'emploi et les employeurs afin de faciliter la transmission respectivement des offres et des candidats.

A l'analyse de la demande d'avis la Commission a constaté que l'authentification sur le téléservice n'était possible qu'en utilisant une identité numérique et qu'aucune alternative n'était prévue.

De cette manière, l'identité numérique jusqu'à présent réservée aux monégasques et aux résidents sera étendue à d'autres populations dont les demandeurs d'emploi. Cette hypothèse avait déjà inquiété la Commission, dans sa délibération n° 2019-120 du 18 septembre 2019 portant avis sur la consultation du Ministre d'Etat sur le projet de Loi relative à l'identité numérique, qui s'était interrogée « *sur l'obligation future d'obtenir un identifiant/ identité numérique pour se connecter aux téléservices de l'Administration* ». Ainsi, elle avait alors demandé au responsable du traitement « *qu'il soit toujours possible et expressément prévu que les personnes désirant accéder aux services en ligne puissent le faire de manière autonome, service par service* ».

Dès lors en l'espèce, la Commission a estimé qu'il était uniquement possible de restreindre l'accès à des téléservices par le seul biais d'une authentification de niveau élevé ou substantiel quand s'applique un principe de nécessité. C'est par exemple le cas lors de l'utilisation de données sensibles ou pour proposer une alternative à des démarches qui nécessitent un déplacement dans les locaux de l'Administration.

Par ailleurs, la Commission a constaté que la création d'une identité numérique pour les demandeurs d'emploi utilisera un système biométrique « *dont il convient et il conviendra encore plus de veiller [...] à la qualité du consentement des personnes s'y soumettant. Or forcer l'identité numérique de niveau substantiel pour ce téléservice conditionnera nécessairement le consentement des demandeurs d'emploi à l'utilisation d'une telle technologie, qui ne pourra donc pas être libre, spécifique, éclairé et univoque* ».

La Commission, estimant que « *l'utilisation obligatoire d'une identité numérique ne doit pas résulter d'une simple opportunité mais doit relever d'une nécessité, renforcée en cas de recours à la biométrie, conditions qui ne sont pas réunies en l'espèce* », a demandé au responsable de traitement qu'une alternative d'authentification soit proposée aux personnes concernées.

Enfin, la Commission a indiqué que dans l'hypothèse où à l'avenir d'autres téléservices devaient proposer uniquement l'identité numérique comme moyen d'authentification, elle sera amenée à apprécier la proportionnalité de la mesure au cas par cas.

La modification du traitement de « *Gestion et suivi des conditions d'entrée et de séjours des résidents étrangers de la Principauté* » de la Direction de la Sûreté Publique (DSP)

Le Ministre d'Etat a soumis à l'avis de la Commission la modification dudit traitement, conformément aux articles 7 et 9 de la Loi n° 1.165 du 23 décembre 1993, afin notamment de prévoir un accès en « *recherche restreinte* » par l'Autorité Monégasque de Sécurité Financière (AMSF).

L'ouverture de cet accès était justifié par l'article 50 de la Loi n° 1.362 relative à la lutte contre le blanchiment de capitaux, qui dispose qu'« *Aux fins d'application de la présente loi, le service exerçant la fonction de renseignement financier de l'Autorité reçoit à leur initiative, ou se fait communiquer à sa demande, dans les plus brefs délais, même en l'absence de la déclaration prévue, selon les cas, aux articles 36 et 40, toute information ou tout document en leur possession, nécessaire à l'accomplissement de sa mission, de la part :*

1°) de tout organisme ou personne visé à l'article premier et aux chiffres 1°) et 2°) de l'article 2 ;

2°) de la Direction de la Sûreté Publique, notamment en ce qui concerne les informations d'ordre judiciaire ;

3°) des autres services de l'État et de la Commune, des personnes morales investies d'une mission de service public ou d'intérêt général, et des établissements publics ;

4°) du Procureur Général ou d'autres magistrats du corps judiciaire ;

5°) des organismes nationaux remplissant des fonctions de supervision ;

6°) des organismes professionnels énumérés par arrêté ministériel, à l'exclusion de ceux des professionnels mentionnés à l'article 2 ;

7°) du Conseil de l'Ordre des avocats-défenseurs et des avocats.

(...) ».

La Commission avait constaté ainsi que l'AMSF est fondée à se faire communiquer des informations nécessaires à l'accomplissement de ses missions par la DSP.

Le responsable de traitement indiquait que « *Les utilisateurs externes à la DSP ayant le rôle applicatif « recherche restreinte »* » ne peuvent vérifier uniquement qu'une personne est bien résidente, étant précisé que « *Ce rôle ne donne accès qu'à une seule page (recherche restreinte) et la recherche nécessite trois critères : le nom, le prénom et la date de naissance* ».

En outre, « *Un seul résultat est renvoyé par l'application :*

- *Les données du résident (...) ;*
- *Un message indiquant aucune correspondance si aucune fiche résident ne correspond aux critères ;*
- *Un message demandant à l'utilisateur de contacter la DSP dans le cas où plusieurs fiches résident répondraient aux critères fournis* ».

La Commission a néanmoins considéré que les notions de « *se faire communiquer à sa demande* », et de « *disposer d'un accès* » au traitement, ne sont pas similaires, même si les deux solutions reviennent in fine à disposer d'une information identique. En effet, si les demandes formulées présentent une probabilité forte d'une information ou validation hiérarchique, les consultations sur des accès dévolus peuvent permettre d'effectuer des requêtes indues.

Aussi, la Commission a demandé à ce que les personnes qui délivrent les habilitations au sein de l'AMSF et les transmettent à la DSP soient en retour mensuellement informées des consultations effectuées par leurs personnels afin de pouvoir apprécier la pertinence et l'absence de détournement de la finalité de ces accès.

L'analyse de cette modification a été l'occasion pour la Commission de se repencher sur la collecte par la DSP de « *relevés bancaires* » des personnes concernées, dont la collecte n'avait pas fait l'objet de remarques de sa part au sein de la délibération n° 2021-107 susvisée.

En effet, mentionnée en « *consultation* » uniquement dans la catégorie « *revenu* », la Commission estimait qu'il s'agissait pour un étranger d'avoir la possibilité de montrer son relevé bancaire pour attester en personne de versements d'argents justifiant de ses capacités de ressources.

La CCIN avait ensuite constaté que la DSP sollicitait ces relevés, en remise en main propre ou par transmission e-mail, afin de faire une analyse approfondie des dépenses pour connaitre des liens de l'étranger résident à Monaco en cas notamment de renouvellement de la carte de séjour.

La Commission a donc estimé cette pratique abusive et trop intrusive dans la vie privée des personnes concernées, lesdits relevés pouvant refléter des

dépenses revêtant un caractère intime. Elle a exclu en conséquence toute collecte ou consultation des relevés bancaires par la DSP.

Les traitements dans le domaine de la santé

Les traitements liés au fonctionnement du CHPG

2 traitements soumis par le Centre Hospitalier Princesse Grace (CHPG) ont reçu un avis favorable de la Commission en 2024.

Le premier de ces traitements a pour objet le « *Dossier administratif du patient informatisé* », le volet médical ayant déjà fait l'objet d'un avis favorable par délibération n° 2021-207 du 20 octobre 2021, et a pour but d'assurer l'enregistrement des informations, pièces d'identité et autre pièce probante des patients, de faciliter le suivi desdits patients au sein de l'établissement et de permettre la facturation et le recouvrement.

La Commission a néanmoins recommandé que les accès externes au traitement par le prestataire ne se fassent que sur demande.

Le second traitement a pour finalité « *Dématérialisation des bulletins de paie* » et concerne les salariés ne s'étant pas opposés à la dématérialisation desdits bulletins. Il est mis en œuvre afin de faciliter et fluidifier l'envoi des bulletins de paie aux salariés, conformément à l'Arrêté Ministériel n° 2019-1088 du 20 décembre 2019 relatif au bulletin de paye électronique.

Ses fonctionnalités sont ainsi les suivantes :

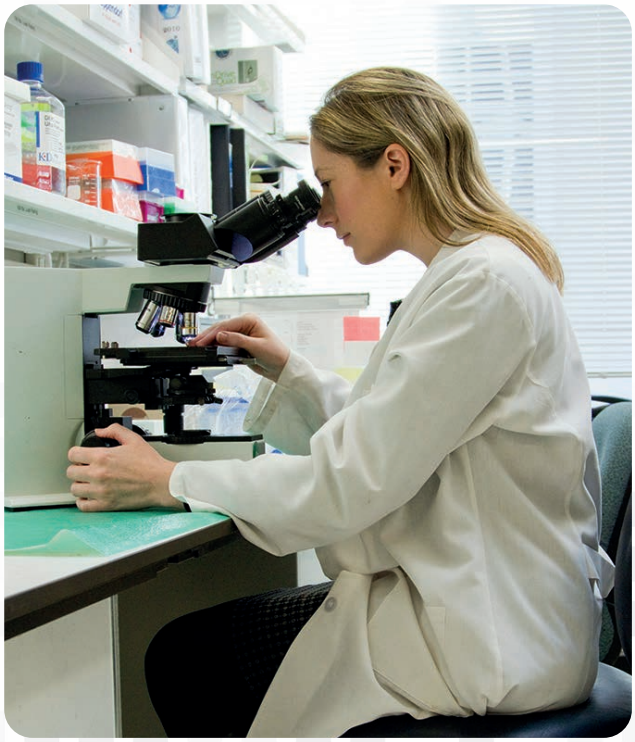
- transmission des bulletins de paie de manière dématérialisée ;
- dépôt des bulletins de paie sur la plateforme de dématérialisation ;
- conservation de documents à valeur probante ;
- déploiement de coffres-forts à destination des salariés ;
- signature des bulletins de paie électroniques via une signature électronique à valeur probante.

Les recherches médicales

Le CHPG a soumis 4 recherches médicales à la Commission pour avis, 2 en tant que responsable de traitement et 2 en tant que représentant d'un promoteur situé en dehors de la Principauté. Ces recherches étaient toutes des études observationnelles qui, préalablement à l'avis favorable de la Commission, ont également reçu un avis favorable de la Direction de l'Action Sanitaire.

La Commission a néanmoins assorti certains de ces avis de remarques sur les mesures de sécurité à mettre en place. Celles-ci étaient les suivantes :

- 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 ;
- si un médecin ou un Attaché de Recherche Clinique devait rejoindre la recherche après son début, l'identifiant et le mot de passe doivent lui être communiqués par deux canaux distincts ;
- la communication des données pseudonymisées chiffrées et des clés de déchiffrement doit être effectuée par deux canaux distincts ;
- les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.



Les traitements issus des réformes en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et la prolifération des armes de destruction massive et la corruption

Entre les modifications de traitements existants et la création de nouveaux traitements permettant la mise en œuvre des différents registres prévus par la Loi n° 1.362, l'évolution des textes entourant la lutte anti-blanchiment, dans une année de revue de la législation monégasque par le GAFI, a conduit à de nombreuses saisines de la CCIN.

Les traitements de l'Autorité Monégasque de Sécurité Financière (AMSF)

- **Sur les conséquences du statut d'Autorité Administrative Indépendante (AAI) de l'AMSF**

L'AMSF étant devenue une AAI qui s'est substituée au Service d'Information et de Contrôle sur les Circuits Financiers (SICCFIN) du Gouvernement, la CCIN a logiquement relevé que les traitements qu'elle met en œuvre utilisent les infrastructures et traitements de l'Etat.

Elle a ainsi souligné que les relations techniques avec le Gouvernement doivent être revues, selon des modalités qui marquent son indépendance, a minima en établissant une relation contractuelle.

- **Sur la gestion du fichier des comptes bancaires et coffres-forts (FICOBAM)**

L'AMSF est chargée par la Loi n° 1.549 du 6 juillet 2023 d'assurer la gestion du fichier des comptes bancaires et coffres-forts (FICOBAM) en application des articles 64-1 et suivants de la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive et la corruption.

Elle ne souhaitait pas informer les personnes concernées de leurs droits, indiquant que les clients des établissements bancaires étaient informés par ces derniers, et que les personnes ayant accès au traitement étaient informées par les dispositions légales.

La CCIN avait cependant rappelé que cela ne dispensait pas l'AMSF d'informer :

- les personnes concernées par le biais de son site Internet de l'existence du présent traitement et des mentions exigées à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;
- les personnels habilités de l'AMSF et des différentes entités prévues dans les dispositions légales via une information directe et conforme aux dispositions de l'article 14 précité.

Le responsable de traitement avait souhaité restreindre le droit d'accès des personnes concernées en le soumettant aux dispositions de l'article 15-1 de la Loi n° 1.165, modifiée, qui encadre le droit d'accès indirect exercé par le biais de la CCIN.

La Commission avait rappelé qu'en application de l'article 64-5 de la Loi n° 1.362, les personnes concernées peuvent exercer l'ensemble de leurs droits auprès de l'AMSF, sous réserve, en cas de rectification nécessaire, d'en faire également la demande à l'établissement bancaire concerné.

Par ailleurs, la demande d'avis précisait qu'ont accès au traitement les agents habilités de l'AMSF ainsi que les personnels des autres entités habilitées à avoir accès, prévus à l'article 64-2 de la Loi n° 1.362.

La Commission constatant que le « *registre est tenu par le service exerçant la fonction de renseignement financier de l'Autorité* » a estimé que seuls les agents habilités de l'AMSF appartenant à ce Service peuvent disposer d'accès aux droits étendus, les autres personnels de l'AMSF ainsi que les personnels habilités des entités tierces ne pouvant avoir accès au traitement qu'en seule consultation.

En outre, il résulte de l'article 54-3 de l'Ordonnance Souveraine n° 2.318 que les personnes sont habilitées, pour leurs personnels respectifs, par le Directeur de l'AMSF, le Directeur des Services Judiciaires, le Directeur de la Sûreté Publique, le Directeur du service de gestion des avoirs saisis ou confisqués. Il est précisé audit article que « *Les personnes qui délivrent ces habilitations tiennent une liste des personnes qu'elles ont habilitées. Elles communiquent cette liste de manière sécurisée au chef du service exerçant la fonction de renseignement financier de l'Autorité* ». Après avoir rappelé que toute modification desdites listes doit être communiquée de manière sécurisée audit Service, la Commission a estimé :

- qu'en cas d'empêchement d'un Directeur, il devrait exister une possibilité d'habiliter les personnels de son entité par le biais d'une délégation de ce pouvoir, délégation qui devrait être textuellement encadrée ;
- que les personnes qui délivrent les habilitations devraient être mensuellement informées, sans que cela n'entraîne une conservation de données supplémentaire et distincte, des consultations effectuées par leurs personnels sur le FICOBAM afin de pouvoir apprécier la pertinence et l'absence de détournement de la finalité de ces accès.

- **Sur la « *Gestion des déclarations de soupçon et des investigations relatives à la LBC-FT-P* »**

L'AMSF a reçu un avis favorable à la modification dudit traitement, qui relève des dispositions de l'article 11 de la Loi n° 1.165. Dès lors, seul le sens de l'avis a été publié.

Les traitements de la Direction du Développement Economique (DDE)

- **Sur les Registres exploités par la DDE**

La DDE a été amenée à modifier ou créer les traitements suivants :

« *Gestion du Registre Spécial des sociétés civiles* » (modification) ;

« *Gestion d'un registre des bénéficiaires effectifs des sociétés commerciales, groupements d'intérêt économique et sociétés civiles de droit monégasque* » (modification) ;

« *Gestion du Registre des Trusts* ».

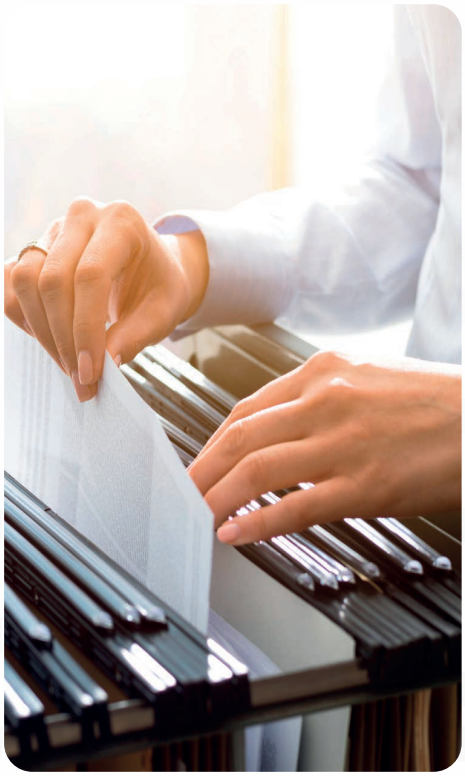
Il a résulté de l'analyse des dossiers une gestion centralisée et transverse des bénéficiaires effectifs présents dans les différents registres. La Commission a demandé au responsable de traitement d'analyser l'impact que ce choix peut avoir sur le plan de la sécurité technique et juridique (par exemple, en cas de dérogation accordée au bénéficiaire effectif le protégeant de l'accès de tiers à ses informations au titre du registre des trust, qu'advient-il si le trust dépasse ensuite 25% dans le capital d'une entité commerciale et que, de fait, le bénéficiaire effectif du trust devient également bénéficiaire effectif de ladite société ?).

La Commission a également identifié un accès en lecture ouvert au Département des Finances et de l'Economie justifié par le responsable de traitement « *dans le cadre de missions transversales avec la DDE en lien avec les activités économiques de la place* ». Elle a cependant relevé l'absence de justification légale et a refusé d'étendre les accès aux registres tels qu'encadrés par les différents textes applicables.

Elle s'est en outre interrogée sur l'étendue des accès dévolus aux entités légalement habilitées et a estimé qu'ils devraient être limités aux seules informations relatives aux bénéficiaires effectifs.

Concernant plus spécifiquement le Registre Spécial des Sociétés Civiles, la question de l'accès ouvert aux Agents de l'Institut Monégasque de la Statistique et des Etudes Economiques s'est également posée.

Le responsable de traitement indiquait qu'en dehors des informations relatives aux agents de la DDE, les informations seraient conservées 10 ans à compter de la date de radiation de l'entité légale, incluant mécaniquement dans ce délai les informations des liquidateurs, avant que soit mise en œuvre une « *restriction des accès au responsable de la section RCI et au directeur de la DDE à des fins historiques, statistiques ou scientifiques en lien avec le SCADA (Service Central des Archives et de la Documentation Administrative) et la MPAN (Mission de Préfiguration des Archives Nationales)* ».



La Commission a relevé que cette durée de « *10 ans à compter de la radiation de l'entité légale* » est légalement prévue pour le RCI et le RSSC, mais que les textes étaient silencieux sur la durée de conservation du Registre des Trusts. Elle a toutefois estimé que cette durée de conservation est cohérente avec les autres dispositions, et les durées de conservation imposées aux entités relativement à leurs bénéficiaires effectifs.

La Commission avait également constaté que des informations sensibles au sens de l'article 12 de la Loi n° 1.165 sont collectées. A cet égard l'article 13-7 de la Loi n° 214 dispose notamment que « *Les restrictions d'accès visées aux alinéas précédents peuvent être sollicitées lorsque le bénéficiaire effectif est un mineur ou est frappé d'incapacité ou lorsque cet accès pourrait exposer le bénéficiaire effectif à un risque disproportionné, un risque de fraude, d'extorsion, de harcèlement, d'enlèvement, de chantage, de violence ou d'intimidation.*

La demande est fondée sur une évaluation détaillée de la nature exceptionnelle des circonstances telles que définies par ordonnance souveraine ».

Lesdites restrictions sont encadrées dans le temps et il est prévu que « *Les dérogations prévues par le présent article ne peuvent être accordées que pour la durée des circonstances qui les justifient sans dépasser une période maximale de cinq ans. Elles peuvent être renouvelées par décision, selon les cas, du Ministre d'État, ou du Président du Tribunal de première instance, à la suite d'une demande de renouvellement motivée du trustee, ou de la personne occupant une position équivalente dans une construction juridique similaire et des bénéficiaires effectifs eux-mêmes* ». La Commission a estimé que le responsable de traitement, à l'issue du délai accordé pour la restriction, peut garder la trace qu'une restriction a été opérée sur une période donnée mais doit supprimer les informations sensibles ayant conduit à cette décision.

Elle a également souhaité appeler l'attention sur la situation des bénéficiaires effectifs qui perdent cette

qualité et dont les informations demeurent conservées sans lien avec la finalité initiale pour cette durée de 10 ans après la dissolution de l'entité légale. Par délibération n° 2020-113 portant avis sur la consultation du Ministre d'Etat relative au projet de Loi renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption il avait été relevé que « *Par ailleurs, la Commission constate que rien ne vient encadrer les durées de conservations des données relatives à un bénéficiaire économique effectif qui perd cette qualité et souligne qu'une durée de conservation spécifique à ce cas d'espèce devrait être prévue* ».

Le responsable de traitement justifiait cette conservation car il « *est nécessaire de pouvoir identifier tous les mouvements se rapportant aux personnes en lien avec les bénéficiaires effectifs et l'entité légale tout au long de la vie de cette entité, puis pendant les années suivant sa dissolution ou sa radiation. Certains de ces mouvements peuvent, par exemple, révéler une organisation, une stratégie de blanchiment ou de dissimulation du véritable BE* ».

La Commission en avait pris acte mais avait relevé que la durée de vie d'une entité légale peut être bien supérieure à toute prescription, voire à l'espérance de vie des personnes concernées, conduisant à des durées de rétention sans lien avec l'objectif recherché. Cet élément vaut pour toutes les personnes concernées dont les informations sont conservées 10 ans à compter de la date de radiation de l'entité légale (tels que notamment les experts-comptables, protecteurs ou encore les documents d'identité des personnels d'établissements bancaires effectuant une demande d'extrait).

De plus, concernant les personnes demandant des informations issues des registres en application des dispositions légales, la Commission a fixé la durée de conservation de leurs informations à 3 ans à compter de la demande.

Enfin, concernant le cas des informations des personnes en charge des informations élémentaires conservées au sein du Registre Spécial des sociétés civiles, la Commission a constaté qu'elles ne sont pas visées comme faisant partie du Registre au sein de la Loi n° 797, précitée, et ne sont pas listées à l'article 10 de l'Ordonnance Souveraine n° 3.573 comme informations élémentaires. En conséquence elle a fixé la durée de conservation des informations relatives aux personnes responsables des informations élémentaires à 5 ans en archive intermédiaire à compter de la perte de cette qualité, avant suppression définitive.

- **Sur la gestion du contrôle de l'activité des entreprises**

Le responsable de traitement avait indiqué dans sa demande d'avis que « *De manière aléatoire, sur une alerte d'un usager, en cas d'identification d'incohérence par les agents d'autres divisions (...) la DCAE [Division du contrôle de l'activité des entreprises de la DDE] organise le contrôle des acteurs économiques* ». Il précisait que « *Les missions de la Division de Contrôle des Activités Economiques (DCAE) de la DDE portent au principal :*

- sur la vérification du respect de l'objet social, soit la cohérence avec les actions réalisées par les entités légales et celles décrites dans leurs déclarations ou autorisations, aboutissant parfois sur le constat d'un dépassement d'objet social ;

- le contrôle de l'affichage des prix ;

- le contrôle de l'activité d'une entreprise qui commence son activité avant d'avoir achevé les formalités de déclaration ou d'avoir reçu l'autorisation d'exercer, selon le cas ;

- la vérification de la qualité du dossier de l'entité : BE déclarés, anomalie dans le dossier, comptes déposés, déclarations quinquennales à jour ... ».

A cette fin, les fonctionnalités sont :

- organisation des contrôles : identification des entités à contrôler, affectation des contrôles aux agents, planification des contrôles ;
- élaboration des documents préparatoires aux contrôles sur pièces ou sur place ;
- rédaction des notes, comptes rendus et rapports relatifs aux contrôles ;
- suivi des correspondances avec les entités légales contrôlées et leurs représentants ;
- enregistrement des doléances ou informations concernant les entités légales exerçant une activité en Principauté ;
- suivi des décisions du Directeur de la DDE ;
- préparation des Commissions de révocation des activités économiques ;
- établissement de statistiques.

Le responsable de traitement souhaitait conserver les dossiers concernant les contrôles :

- 10 ans après la date de liquidation ou de radiation de l'entité légale ;
- puis restriction des accès au responsable du Pôle Conformité, Contrôle et Enregistrement et au Directeur de la DDE à des fins historiques, statistiques ou scientifiques en lien avec le SCADA (Service Central des Archives et de la Documentation Administrative) et la MPAN (Mission de Préfiguration des Archives Nationales).

Il précisait que « *Cette durée de conservation est nécessaire car elle permet dans le temps, par exemple :*

- *De suivre le respect de la règlementation par une entité légale ou ses représentants successifs dans le temps ;*
- *D'éviter que par différents montages juridiques, une personne ne tente de créer une activité alors que cette activité a fait l'objet d'un refus d'autorisation ou d'une révocation ;*
- *De s'assurer qu'une personne contrôlée en dépassement d'objet social ne tente par ailleurs d'être autorisée à exercer une activité similaire, potentiellement révocable car en dépassement d'objet* ».

La Commission avait toutefois relevé que les durées de conservation évoquées étaient trop longues eu égard aux justifications avancées, s'alignant sans justification à la durée d'existence de l'entité objet de la vérification (ou de la vérification de son bénéficiaire effectif), et donc sans lien avec le contrôle opéré. Elle a donc fixé la durée de conservation, si les informations ne sont pas anonymisées à plus brève échéance, à 5 ans à compter de la clôture définitive du dossier.

- **Sur la mise en œuvre de la modification du traitement automatisé d'informations nominatives ayant pour finalité « *Permettre la consultation d'informations et l'achat d'extraits du Répertoire du Commerce et de l'Industrie et du Registre Spécial des Sociétés Civiles par voie dématérialisée* »**

Les fonctionnalités du traitement sont :

- diffusion des informations du RCI et/ou du RSSC pouvant être accessibles en ligne ;

- gestion des achats d'extraits du RCI et/ou du RSSC ;
- permettre aux demandeurs d'accéder à leur historique d'achats ;
- gestion du Back Office du site internet ;
- gestion du Back Office du paiement en ligne ;
- diffusion d'un lien vers la liste d'entités légales en déshérence ;
- analyse de données.

La DDE souhaitait conserver les informations relatives aux usagers commandant des extraits pendant 10 ans, « *durée de conservation validée par la CCIN en 2006* », excepté les données de cartes bancaires et les données permettant l'identification de la localisation de l'opération d'achat qui sont conservées 15 mois. A cet égard, la Commission a considéré cette durée excessive. En ce qui concerne les informations liées à l'usager, elle a rappelé que ce téléservice ne doit pas étendre les durées de conservation encadrées par le traitement ayant pour finalité « *Gestion du compte permettant aux usagers d'entreprendre et suivre des démarches par téléservices* », qui sont de trois ans à compter de la dernière connexion. Pour les informations de paiement et facturation, la Commission a fixé leur durée de conservation à 5 ans.

Les traitements du secteur privé : focus sur des problématiques spécifiques

Le recours aux messageries instantanées dans le domaine bancaire

La Commission a été saisie de trois demandes d'autorisation relatives à la mise en place, par des établissements bancaires, d'outils de messagerie instantanée pour la passation d'ordres en plus des canaux de communication classiques généralement déployés au sein des établissements bancaires.

Ainsi, en 2024 la Commission s'est prononcée sur la passation d'ordres *via* :

Bloomberg (deux demandes d'autorisation) : l'entreprise américaine propose un service d'emailing ainsi que de messagerie instantanée (chat) ;

une interface bancaire reliée au WhatsApp du client (une demande d'autorisation) : l'application de messagerie est utilisée par un établissement bancaire de la Place dans le cadre de la souscription à l'offre « *E-services* » pour les clients qui le souhaitent. Concrètement dans le dossier soumis à autorisation,

le client concerné pouvait échanger avec son gestionnaire « *par le biais d'un canal sécurisé utilisant l'application WhatsApp (côté client) et une interface web dédiée et sécurisée (côté gestionnaire)* ».

Il a été constaté que ces messageries instantanées étaient souvent dotées d'une surcouche logicielle de contrôle Data Leak Prevention (DLP).

A cet égard, la Commission a attiré l'attention des responsables de traitement en indiquant que ce type de traitement ne doit pas conduire à une surveillance permanente et inopportune des salariés. Ainsi, elle a exclu du périmètre d'un des traitements soumis à son autorisation une fonctionnalité qui permettait au responsable de traitement de contrôler par échantillonnage l'activité des salariés et les règles « *Groupe* » de communication. En effet, la Commission a estimé ne pas être en mesure de se prononcer sur cette fonctionnalité qui recouvrait « *des domaines dont le périmètre est difficilement appréhendable notamment s'agissant des règles Groupe de communication* ».

S'agissant de l'information des personnes concernées, la Commission a souligné que celle-ci devait être différente selon que la personne concernée était un client ou un salarié de la société.

Ainsi, pour l'information des clients la Commission considère que le seul renvoi aux Conditions Générales ne constituait pas une information conforme au regard de l'article 14 de la Loi n° 1.165. Toutefois, dans le dossier soumis à analyse, le responsable du traitement informait les clients, préalablement à l'utilisation de ce canal, au moyen d'un document spécifique à savoir

les conditions d'utilisation de l'outil. De plus, le client devait non seulement lire mais également accepter ces conditions.

En ce qui concerne l'information des salariés, la Commission considère que ces derniers doivent être informés du traitement de leurs données dans le cadre des présents traitements. De plus, cette information doit non seulement comprendre l'ensemble des éléments listés à l'article 14 de la Loi n° 1.165 mais également, lorsque l'outil dont s'agit est soumis à un contrôle/supervision DLP, ils doivent recevoir communication des règles d'utilisation de l'outil et l'information de l'existence de ce contrôle afin d'être en mesure d'adapter leur comportement.

Le contrôle périodique des salariés

Un établissement bancaire souhaitait effectuer des contrôles périodiques d'un nombre limité d'employés identifiés comme occupant des postes sensibles portant sur les casiers judiciaires ainsi que de potentiels évènements liés aux risques de criminalité financière.

Le responsable de traitement indiquait que le traitement est justifié par le respect d'une obligation légale à laquelle il est soumis, par l'exécution d'un contrat avec la personne concernée ainsi que par la réalisation d'un intérêt légitime, sans que ne soient méconnus les droits et libertés fondamentaux de la personne concernée.

La Commission a écarté la justification sur l'obligation légale, relevant qu'il n'y a pas en droit interne de dispositions qui obligeraient un salarié de banque à transmettre obligatoirement son casier judiciaire, comme celle fondée sur l'exécution d'un contrat, qui n'était étayée d'aucun élément au dossier.

Elle a néanmoins relevé que la banque disposait d'un intérêt légitime à procéder aux vérifications objets du présent traitement, eu égard au secteur particulier dont s'agit qui nécessite une gestion des risques et des garanties quant à la prévention de tout acte en lien avec des infractions de corruption ou financières

La Commission rappelait que l'application d'analyses en lien avec la lutte contre le blanchiment de capitaux portant sur des salariés n'est expressément prévue que lors de la procédure d'embauche et constatait qu'en ce qui concerne l'organisation interne, la soumission des personnels des établissements bancaires aux vérifications n'est pas expressément prévue en Principauté.

Elle a relevé toutefois que des procédures doivent être mises en place eu égard aux risques de blanchiment et de corruption mais a estimé, conformément aux dispositions de la Loi n° 1.362, que ces vérifications doivent en tout état de cause s'opérer eu égard au niveau de responsabilité exercé et au risque pesant sur la relation d'affaires, relativement au blanchiment et au risque de corruption. A cet égard, la Commission a relevé que les

opérations de vérifications concernent des personnels identifiés comme étant « *sensibles* », recensés sur une liste faisant l'objet d'une revue annuelle.

Par ailleurs, la Commission constatait que le traitement opérait une différence de traitement entre les salariés résidents français (entendu comme salariés résidents en France) et les autres.

Il était en effet indiqué, « *concernant les employés non-résidents français* », que le prestataire qui effectue les vérifications pour le compte de la banque « *effectue les demandes auprès du service gouvernemental afin d'obtenir le casier judiciaire. Il procède par la suite à la vérification de celui-ci* ».

A contrario, concernant les salariés résidents en France, la banque ne pouvait qu'analyser les casiers transmis par les salariés.

La Commission a demandé que le régime appliqué aux salariés résidents en France soit appliqué à l'ensemble des employés, en l'absence de justification particulière et a estimé que les personnes concernées devaient être informées des éventuelles conséquences si elles choisissaient de ne pas communiquer leur casier judiciaire.

En effet, cette situation n'était envisagée que sous le prisme d'un risque « *d'escalade* » alors qu'il est indiqué au sein d'une annexe que « *toutes les données sont collectées et utilisées uniquement dans le but de réaliser la prestation (vérification des antécédents d'un candidat) et avec le consentement de la personne concernée* ». N'étaient en effet indiquées au dossier que les seules conséquences qu'un salarié encourt en cas d'écart majeur entre les éléments qu'il fournit et les constatations opérées par la banque, à savoir :

- demander des explications à l'employé concerné ;
- contacter les services locaux Ressources Humaines et Compliance & Operational Risk Control pour information et demande de préconisation ;
- prendre les mesures adéquates (un changement de poste ou une restriction d'accès).

La Commission a en outre rappelé qu'il devait y avoir une certaine corrélation entre la nature de la condamnation de l'employé et son métier au sein de la banque, toute condamnation ne devant pas entrainer par principe des conséquences à son égard.

Le filtrage et la notation des fournisseurs

La CCIN a autorisé un établissement bancaire à procéder à l'analyse des documents et informations relatives à des prestataires/fournisseurs afin d'établir le risque avant l'entrée en relation avec ceux-ci, ainsi que, de manière périodique, tout au long du contrat.

Après avoir relevé qu'aucune disposition de la Loi n° 1.362 du 3 août 2009, modifiée, n'impose la mise en place de mesures de vigilance à l'égard des fournisseurs et des prestataires, la Commission a demandé au responsable de traitement « *que seules les personnes morales soient concernées par la mise en place des mesures de vigilances issues du présent traitement* ».

De plus, elle a précisé « *que des personnes physiques dont les informations sont publiques et liées à la structure vérifiée peuvent indirectement être concernées [...], lorsqu'elles ressortent des recherches effectuées, tels que les représentants des personnes morales* ».

Enfin, la CCIN a estimé que ce traitement ne pouvait pas permettre de « *soumettre à la vérification l'ensemble des personnels des entités vérifiées qui entrent en interaction avec la Banque* ».

Quid des données relatives à la vitesse, au temps de conduite ou encore aux pauses des conducteurs de véhicules de transport routier

En 2024, la CCIN a autorisé trois traitements relatifs à la collecte des activités de conduite des conducteurs de transport routier provenant des appareils de contrôle de vitesse, dits chronotachygraphes, installés dans leurs véhicules professionnels.

Ces données peuvent en effet être collectées en Principauté mais non dans le cadre d'un traitement lié aux données de géolocalisation du véhicule mais plutôt dans le cadre d'un traitement lié à la collecte et l'archivage des données des chronotachygraphes numériques installés dans les véhicules poids lourds. Ce traitement est alors justifié par une obligation légale à laquelle est soumis le responsable de traitement.

L'article 1 de l'Arrêté Ministériel n° 90-651 du 28 décembre 1990 relatif à l'utilisation des appareils de contrôle de vitesse (chronotachygraphes) des véhicules automobiles dispose en effet que « *Tout véhicule automobile dont le poids maximal autorisé, avec ou sans remorque, est supérieur à 3,5 tonnes doit être équipé d'un appareil de contrôle de vitesse dît chronotachygraphe* ».

De plus, l'article 2 dudit Arrêté Ministériel dispose que « *Les chronotachygraphes doivent [...] permettre l'enregistrement, en sus de la vitesse des véhicules, des éléments suivants : - distance parcourue ; - temps de conduite ou autre temps de travail ; - interruption de travail et temps de repos journalier ; - ouverture du boîtier contenant la feuille d'enregistrement* ».

Enfin, le Règlement (CEE) n° 561/2006 du Parlement et du Conseil du 15 mars 2006 relatif à l'harmonisation de certaines dispositions en matière sociale dans le domaine de transports par route « *fixe les règles relatives aux durées de conduite, aux pauses et aux temps de repos qui doivent être observés par les conducteurs assurant le transport de marchandises et de voyageurs par route* ».

Aux termes de son article 2, il est applicable quel que soit le pays d'immatriculation du poids lourd, dès lors qu'il circule sur le territoire de la Communauté Européenne.

Les refus d'autorisation et les avis défavorables de la Commission

Le réseau social interne à l'Administration

La Direction des Services Numériques (DSN) a soumis à la Commission une demande d'avis relative au traitement dont la finalité est « *Gestion du réseau social de l'Administration Monégasque : Workplace* » et qui a pour objectif de mettre à disposition des fonctionnaires et agents un espace dédié à la diffusion des informations et de permettre la constitution de groupes transversaux entre les différents Services et Départements.

En 2019, ledit traitement avait fait l'objet d'un avis défavorable de la CCIN en raison de l'absence de précisions concernant le ou les transferts de données issus de l'exploitation de ce réseau social qui s'appuyait sur une architecture Facebook.

Une version modifiée de la demande d'avis a été soumise à l'avis de la CCIN en 2024. A l'analyse de celle-ci, la Commission a constaté que les remarques formulées en 2019 ont majoritairement été intégrées avec notamment l'encadrement de l'exploitation des données par Meta ainsi que le sort des données à la fin du contrat.

De plus, la demande d'avis était accompagnée d'une demande d'autorisation de transfert de données. Toutefois, à l'étude des garanties appropriées mises en place par le responsable de traitement pour encadrer le transfert de données aux Etats-Unis, la Commission a considéré qu'elle n'était pas en mesure de se prononcer sur le transfert de données à Meta en se référant aux informations qui lui ont été communiquées. En effet, elle a constaté qu'aucune disposition du contrat signé entre les parties n'encadre spécifiquement ce transfert d'in-

formations et que les clauses contractuelles conclues ne peuvent être retenues en raison de leurs incohérences intrinsèques.

De plus, la Commission a relevé que différents types de cookies étaient exploités dans le cadre dudit traitement, ce qui conduisait le responsable de traitement à procéder à au moins un transfert de données supplémentaire vers les Etats-Unis, alors qu'aucune demande d'autorisation en ce sens ni précision sur ces éventuels transferts n'a été communiquée.

En conséquence, la Commission a rappelé que conformément à l'alinéa 1er de l'article 14-2 de la Loi n° 1.165 l'utilisateur doit bénéficier d'une « *information claire et complète (...) sur la finalité du traitement et sur les moyens dont il dispose pour s'y opposer* ». Elle a enfin rappelé que le responsable de traitement ne peut faire peser le consentement aux cookies sur une information de l'utilisateur quant au possible paramétrage de son navigateur.

Ainsi, la Commission a émis un avis défavorable à la mise en œuvre dudit traitement.

Un traitement LAB non conforme, et un transfert au périmètre incertain

La Commission a refusé la mise en œuvre d'un traitement en matière de lutte contre le blanchiment de capitaux, et une demande d'autorisation de transfert associée.

L'examen de ce dossier a mis en lumière un défaut de maîtrise en matière de quantum d'informations collectées, de finalité exacte du traitement et de modalités d'exercice des droits, qui ne peuvent se faire que de manière indirecte au cas d'espèce.

S'agissant du transfert associé, la Commission n'a pas été en mesure de déterminer le périmètre exact de ce transfert, à savoir : les catégories de destinataires, leurs lieux exacts d'implantation, ainsi que les finalités précises de ce transfert. Elle a ainsi mentionné au sein de sa délibération :

« *Toutefois, l'objectif du transfert n'est pas spécifiquement identifié. Dès lors, la Commission considère que la finalité du transfert d'information n'est ni déterminée, ni explicite. En effet, si le responsable de traitement indique que les informations sont transmises « au département informatique de la société mère » il appert néanmoins à l'analyse de la demande d'autorisation de transfert que d'autres catégories de personnes (internes ou externes à la société) situées dans un pays ne disposant pas d'un niveau de protection adéquat peuvent accéder aux données des différents traitements concernés par ce transfert. Ainsi, il semble à la Commission que le transfert déposé ne se limite pas à une finalité qui concerne plusieurs traitements (exemple : transfert à des fins d'hébergement), mais bien plusieurs finalités de transfert concernant plusieurs traitements.* »

7

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.

La CCIN s'affiche sur LinkedIn pour la Journée de la Protection des Données Personnelles

Pour la 18ème Journée de la Protection des Données Personnelles, célébrée comme chaque année le 28 janvier, la CCIN a décidé de créer sa propre page LinkedIn afin de présenter ses actualités ainsi que les derniers développements en matière de protection des données tant en Principauté qu'au niveau européen.

Cette page est alimentée régulièrement. N'hésitez donc pas à la suivre !

Réunion de lancement de Groupes de travail avec les Banques

Fort du constat partagé entre les établissements bancaires et la CCIN de l'existence de questionnements récurrents sur les traitements qu'ils mettent en œuvre, s'est tenue le lundi 18 mars 2024 une réunion ayant pour objectif d'instaurer des Groupes de travail thématiques sur les différents points identifiés. Le but de cette démarche est, à court terme, de répondre à ces interrogations et d'harmoniser les pratiques au sein d'un document commun, et à long terme, si les associations et les organismes professionnels représentant ce secteur le désirent, que ce document serve à élaborer un Code de conduite, nouvel outil de conformité instauré par la Loi n° 1.565 relative à la protection des données personnelles.

Dans le prolongement de cette présentation du 18 mars, les Groupes de travail thématiques se sont réunis à plusieurs reprises entre le 7 juin et le 21 novembre 2024 dans les locaux de l'Association Monégasque des Activités Financières (AMAF) afin d'échanger sur les thématiques exposées lors de la réunion de lancement.

Ces Groupes de travail ont abordé plusieurs sujets tels que les traitements relatifs à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive et la corruption, les durées de conservation, les mesures de sécurité.

De plus, à cette occasion la CCIN est revenue sur les contours de l'obligation d'information concernant les personnes concernées par un traitement de données et ses conséquences en termes de formalités de l'introduction de nouvelles normes, notamment européennes.

En outre, les discussions ont porté sur les pratiques informatiques du secteur bancaire et sur le niveau de sensibilisation face aux enjeux liés à la sécurité numérique. Enfin, les 11 juin et 10 juillet 2024, le recours à des dispositifs d'alerte, des outils et d'échanges intra-groupes par les entités financières ont également permis au Groupe de travail d'aborder les problématiques liées aux transferts de données personnelles hors de la Principauté.

Merci à l'AMAF et à l'Association Monégasque des Compliance Officer (AMCO) pour leur contribution à l'organisation de ces réunions et pour leur participation, dont l'objectif est de fédérer le secteur bancaire.

Les Sociétés de gestion ont été associées à cette démarche tout en prenant en compte leurs spécificités, notamment en termes de moyens humains.

Organisation à Monaco d'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

Le 21 mars 2024, la CCIN a accueilli à Monaco, pour la deuxième année consécutive, 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 (« *GT AID* ») dont elle assure la Vice-Présidence.

L'objectif de cette réunion était de préparer le panel « *action humanitaire et protection des données* » que le GT AID a organisé lors du Symposium de Venise en juin 2024 et de discuter des projets à mener au cours de l'année.

Plusieurs actions ont ainsi été identifiées dont notamment la création d'une liste, illustrée d'une carte, des points de contacts au sein des Autorités de protection des données sur le continent africain, la mise à jour d'une cartographie géographique et thématique des acteurs pertinents du secteur humanitaire et l'organisation d'une table ronde avec des Agences de développement.

Etaient présents à cette réunion pour les Autorités de protection des données, le Préposé fédéral à la protection des données et à la transparence (PFPDT) - Suisse, Président du Groupe, l'Agence de Protection des données à caractère personnel – Croatie, l'Autorité pour la protection des données et de la vie privée (APDPVP) – Gabon, le Service de protection des données personnelles (PDPS) - Georgie, et la Commission Nationale pour la Protection des Données (CNPD) – Luxembourg, et pour les organisations internationales, le Comité International de la Croix-Rouge (ICRC), le Haut-Commissariat des Nations Unies pour les Réfugiés (UNHCR) et l'Organisation Internationale pour les Migrations (IOM).

Présence de la CCIN au Forum Incyber autour du thème : « *Ready for AI ? Réinventer la cybersécurité à l'ère de l'IA* »

C'est dans un contexte marqué par l'essor de l'intelligence artificielle (IA) que s'est déroulée du 26 au 28 mars 2024 à Lille la 16ème édition du forum Incyber autour du thème : « *Ready for AI ? Réinventer la cybersécurité à l'ère de l'IA* ».

Ce rendez-vous annuel important pour un grand nombre d'acteurs de la cybersécurité a eu lieu à quelques mois des Jeux Olympiques et Paralympiques de Paris 2024 et de l'entrée en vigueur de la directive NIS visant à renforcer la cybersécurité au sein de l'Union européenne.

La CCIN était présente au forum Incyber pour rencontrer des experts en cybersécurité et échanger sur les thèmes afférents à la sécurité des réseaux, la sécurité des terminaux et des applications ou encore les opérations de sécurité lors de scénarios de cyberattaques.

Lors de cette édition tous les participants ont pu se rendre compte des bouleversements engendrés par l'IA dans un contexte marqué par une croissance permanente des données numériques sur la cybersécurité.

Durant ces trois jours d'échanges professionnels marqués par des ateliers, des démonstrations et des conférences, la CCIN a pu assister lors du sommet d'ouverture à la première Plénière. Thierry Breton, ancien Commissaire européen au marché européen s'est exprimé sur les enjeux européens face à l'IA en déclarant que « *l'intelligence artificielle va être un moyen de lutter contre des attaquants qui sont eux-mêmes équipés d'intelligence artificielle. À court terme, cela va permettre d'automatiser, de massifier et de rendre la menace plus sophistiquée* » tout en soulignant que l'IA « *ne changera pas seulement nos process et notre manière de travailler. Elle nécessitera également une adaptation des personnes, des salariés. Cela devrait être mutualisé et partagé à l'échelle mondiale, et je crois que ce forum est un excellent endroit pour le faire* ».

La seconde plénière s'est tenue autour du sujet « *Révolution numérique et de basculements géopolitiques : l'Europe est-elle toujours dans la course ?* » afin de mettre en évidence les défis mondiaux actuels dus à l'augmentation constante des cyberattaques de plus en plus graves et critiques auxquelles les infrastructures européennes doivent faire face.

A ce sujet, Hugues Foulon le CEO d'Orange Cyberdéfense, a pu souligner que « *nous sommes témoins d'une révolution numérique permanente, rapide, accélérée, qui touche nos sphères privées, professionnelles, et même notre vie citoyenne. La digitalisation va à une telle vitesse, avec des bienfaits évidents, que nous avons peut-être tendance à oublier les risques associés et le côté obscur de la force* ».

Cette année, les préoccupations autour de l'IA et ses enjeux tant juridiques qu'opérationnels ont pu enrichir les débats et ouvrir les réflexions sur un sujet plus qu'actuel : l'IA est-elle fiable ? Respecte-t-elle notre vie privée ? Est-elle éthique ?

Ce sont des questions qui devraient trouver des réponses dans les années à venir...

Déplacement à Washington DC pour l'atelier des organisations internationales sur la protection des données

Fin septembre, un agent du secrétariat s'est rendu, à l'invitation du Comité européen à la protection des données (CEPD), à Washington DC, afin de participer à l'atelier des organisations internationales sur la protection des données.

Co-organisé avec la Banque mondiale, cet évènement qui a fêté en 2024 son 20ème anniversaire, a été l'occasion de rencontrer près de 170 représentants d'organisations internationales et de discuter de leurs expériences, meilleures pratiques, défis et préoccupations concernant la protection des données dans le cadre de leurs activités.

De nombreux sujets ont ainsi été évoqués dont notamment le développement et l'utilisation de l'intelligence artificielle, les transferts de données vers et entre les organisations internationales ainsi que la prévention, l'atténuation et la réponse aux violations de données personnelles ou encore la conformité des outils informatiques.

La CCIN a célébré le « *Cybermonth* » en publiant 6 fiches mémo sur la sécurité numérique

Chaque année, le mois d'octobre est le mois de la sensibilisation à la cybersécurité et en 2024 la CCIN s'est jointe à cette initiative mondiale en publiant 6 fiches mémo pour aider les particuliers à assurer leur sécurité numérique.

6 thèmes sont ainsi abordés : Internet, les réseaux sociaux, les cookies, le Wifi, la téléphonie mobile et la messagerie instantanée.

Alors que nous dépendons tous aujourd'hui de la technologie pour mener notre vie personnelle et professionnelle, il est en effet plus important que jamais de connaitre les risques que celle-ci entraîne et de prendre des mesures proactives pour se protéger.

Déclaration commune sur l'extraction de données et la protection des renseignements personnels

Plusieurs Autorités de protection des données, dont la CCIN, ont publié le 28 octobre 2024, une déclaration commune finale sur l'extraction de données (« *data scraping* ») qui explique de quelle façon les entreprises de médias sociaux peuvent mieux protéger les renseignements personnels, compte tenu des préoccupations croissantes suscitées par l'extraction massive de données personnelles provenant des plateformes de médias sociaux, notamment pour soutenir les systèmes d'intelligence artificielle.

Ce document fait suite à une précédente déclaration publiée en 2023 par certaines de ces Autorités, qui traitait des principaux risques pour la vie privée que présente l'extraction de données, c'est-à-dire l'extraction automatisée de données à partir du Web, y compris des plateformes de médias sociaux et d'autres sites Web qui hébergent des renseignements personnels accessibles au public.

Les Autorités de protection des données avaient alors demandé à l'industrie de cerner et de mettre en œuvre des mesures de contrôle pour se protéger contre l'extraction de données provenant de leurs plateformes, les surveiller et y réagir, notamment en prenant des mesures pour détecter les activités des robots et bloquer les adresses IP lorsque des activités d'extraction de données sont détectées.

La déclaration finale, rédigée après un dialogue constructif engagé entre les Autorités de protection des données et plusieurs de ces entreprises de médias sociaux, fournit des directives supplémentaires pour aider les entreprises à s'assurer que les renseignements personnels de leurs utilisateurs sont protégés contre l'extraction illégale de données.

Parmi ces nouvelles attentes, figurent notamment :

- Se conformer aux lois sur la protection des renseignements personnels et des données lorsqu'elles utilisent des renseignements personnels (y compris ceux provenant de leurs propres plateformes) pour élaborer de grands modèles de langage à l'aide de l'intelligence artificielle ;
- Déployer une série de mesures de protection combinées, les réviser et les mettre à jour régulièrement pour tenir compte de l'évolution des techniques et des technologies d'extraction ;
- S'assurer que l'extraction de données à des fins commerciales ou socialement bénéfiques est légitime et conforme à des modalités contractuelles strictes.

Participation à Jersey aux réunions annuelles de l'AMVP et de l'AFAPDP

Du 28 ottobre au 1er novembre 2024, un agent du Secrétariat a participé à la 46ème conférence de l'Assemblée mondiale pour la protection de la vie privée (AMVP et à la 16ème assemblée générale et extraordinaire de l'AFAPDP qui se sont tenues aux larges des côtes françaises, à Jersey.

Les deux premiers jours de l'AMVP, lors des sessions ouvertes, de nombreux débats, discussions de groupe et évènements parallèles ont été organisés autour du thème principal *« the power of i » (le pouvoir du i) décliné en 8 sous-thèmes « Individus, Innovation, Information, Intégrité, Indépendance, International, Interculturel et Indigène »* afin d'explorer le respect et l'équilibre du pouvoir de l'information avec la nécessité pour les citoyens du monde entier d'avoir le pouvoir, le contrôle et la dignité sur leurs informations personnelles.

Ces sessions ouvertes ont été suivies de 2 jours de conférence fermée réservée aux Autorités de protection des données.

Par ailleurs, la veille de ce grand évènement annuel, l'Association francophone des autorités de protection des données personnelles (AFAPDP) a profité de la venue sur l'ile anglo-normande de nombreuses délégations francophones pour organiser à Saint-Hellier son assemblée générale et extraordinaire qui a permis d'adopter la révision de ses statuts et d'élire sa nouvelle Présidente, Madame Drudeisha Madhub, Commissaire à la protection des données de l'Office de protection des données de Maurice.

Créée en 2007 à Montréal, l'AFAPDP a pour but de susciter le débat sur les enjeux de la protection des données personnelles au sein de la Francophonie ainsi qu'à promouvoir l'établissement d'un réseau d'échange et de coopération entre les Autorités indépendantes chargées de la protection des données.

Intervention lors du Diplôme interuniversitaire de Droit Monégasque

Créé en 2024 à l'initiative du Professeur Strickler, Directeur scientifique de l'Institut Monégasque de Formation aux Professions Judiciaires, le Diplôme interuniversitaire de Droit Monégasque est ouvert aux étudiants des universités de Nice et d'Aix en Provence.

Une séance de formation a été consacrée aux Autorités Administratives Indépendantes de la Principauté. C'est dans ce cadre que les représentantes de la Commission de Contrôle des Activités Financières (CCAF), de l'Autorité Monégasque de Sécurité Financière (AMSF) et de la CCIN ont été invitées à présenter leurs Autorités respectives, les raisons ayant conduit à leur création, leurs missions, ainsi que leur fonctionnement.

Cette session de formation s'est tenue le 28 novembre 2024, date du vote de la Loi ayant substitué l'APDP à la CCIN, ce qui a été l'occasion de revenir sur les 31 années d'existence de la CCIN, en évoquant sa création, l'évolution de son statut, et le rôle à venir de l'APDP.

Mesdames Magali VERCESI, Secrétaire Général de la CCAF ; Agnès LEPAULMIER, Secrétaire Général de la CCIN et Sophie THEVENOUX, Directeur de l'AMSF

APDP
AUTORITÉ DE PROTECTION
DES DONNÉES PERSONNELLES

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