CCIN

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

RAPPORT D'ACTIVITÉ 2021

13ème rapport public

Le message du Président

Chaque année davantage le sentiment d'être abreuvés d'un flux continu d'informations - tantôt graves, tantôt futiles, les révélations d'Edward Snowden sur la surveillance de masse, la crise sanitaire, désormais la guerre en Europe - nous questionne sur l'équilibre de notre société, notre place en son sein, et le respect de nos libertés et droits fondamentaux.

Il semble s'agir d'un tiraillement de fond, dans un contexte d'urgence permanente, qui touche par essence la protection des données personnelles. Il n'est donc pas étonnant que le présent rapport d'activité en soit le reflet.

L'activité de la Commission et de ses Services a en effet été particulièrement soutenue en 2021, toujours marquée par les effets de la crise sanitaire, mais aussi par le fort accroissement des dossiers de formalités préalables qui lui ont été soumis, des plaintes qui lui ont été adressées et des saisines par le Ministre d'Etat sur des projets de textes législatifs ou réglementaires.

Ces dernières ont très souvent été faites dans l'urgence, si ce n'est parfois a posteriori, conduisant notre Commission à se demander si la protection des données personnelles est appréhendée comme une opportunité, ou comme une contrainte.

Il s'agit donc pour chacun de placer un curseur sur le degré de protection des données qu'il estime nécessaire et suffisant. Une balance des intérêts qui se trouve au cœur du projet de Loi relative à la protection des données personnelles, dont l'objet est d'introduire en droit interne les standards internationaux régissant la matière, et dont la teneur déterminera le niveau de protection offert par Monaco dans ce domaine.

En fin d'année 2020, notre Commission avait rendu un avis sur une première version de ce projet. Elle avait notamment alerté sur les choix gouvernementaux qui risquaient d'éloigner la Principauté d'un cadre équilibré et, dès lors, de mettre en péril l'objectif affiché d'obtenir une décision d'adéquation de la Commission européenne.

Au cours de l'année écoulée, trois réunions ont été tenues avec le Ministre d'Etat, destinées principalement à évoquer ces problématiques. Si nous avons retenu des échanges avec le Ministre d'Etat une volonté certaine de tenir compte de nos remarques, il n'en demeure pas moins que le projet de Loi tel que déposé au Conseil National en fin d'année 2021 n'adresse pas la majeure partie des préoccupations de la CCIN, dont celles revêtant une acuité particulière à l'aune des dispositions qui serviront de référence lors de l'évaluation du niveau de protection offert par le droit interne en matière de traitement des données personnelles.

Les autres dossiers évoqués avec le Ministre d'Etat ont également permis de mettre en évidence son souhait d'être dans une certaine mesure à l'écoute des remarques de la CCIN. Tel a été le cas concernant la collecte de données de santé dans le cadre de la crise sanitaire, les conditions d'exploitation des caméras de vidéo-protection urbaine, ou encore le recours à l'utilisation des drones par la Direction de la Sûreté Publique.

Comme ailleurs, ce tiraillement de fond se fait également ressentir en Principauté. La nécessité d'une intervention de notre Commission pour que les principes de base de la protection des données personnelles et du respect de la vie privée soient pris en compte par les services exécutifs de l'Etat dénote en effet d'une imprégnation insuffisante de la matière. A l'inverse nous constatons de la part de certains services gouvernementaux et d'entités privées une réelle volonté de placer la protection des données au cœur de leur processus décisionnel.

Je ne peux donc qu'appeler de mes vœux que les bonnes pratiques mises en place par certains services soient plus largement étendues, et que la protection des données personnelles soit reconnue comme étant un élément essentiel ne conduisant pas à abaisser le haut niveau de sécurité désiré par la Principauté.

Le développement d'un écosystème numérique nécessite l'adhésion des utilisateurs, qui ne peut s'obtenir qu'avec la pleine confiance dans la bonne utilisation de leurs données personnelles.

Puissions-nous espérer qu'à l'avenir la CCIN soit associée plus en amont par le Gouvernement afin d'être en mesure d'exposer de manière efficiente les enjeux sociétaux de la protection des données personnelles.

Guy MAGNAN

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

Sommaire

Sommaire

LA COMPOSITION DE LA COMMISSION

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

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

Suite au décès de Monsieur Jean Yves PEGLION survenu en début d'année 2021, Monsieur Robert CHANAS a été nommé Commissaire par Ordonnance Souveraine n° 8.575 du 25 mars 2021, sur proposition du Conseil Communal, pour la durée restant à courir du mandat de son prédécesseur.

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

GUY MAGNAN

Président

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

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

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

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

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

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

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

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

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

RAINIER BOISSON

Vice-Président

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

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

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

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

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

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

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

Florestan BELLINZONA

Commissaire

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

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

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

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

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

Philippe BLANCHI

Commissaire

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

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

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

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

Robert CHANAS

Commissaire

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

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

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

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

La même année, il devient Agent Comptable.

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

Jean-François CULLIEYRIER

Commissaire

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

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

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

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

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

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

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

01

LES MISSIONS ET LE FONCTIONNEMENT DE LA COMMISSION

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

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

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

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

UNE MISSION D'INFORMATION

Au travers de la publication :

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

UNE MISSION DE CONTRÔLE

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

Dans ce cas a été prévue la possibilité pour les responsables de locaux professionnels privés de faire valoir leur droit de s'opposer aux opérations d'investigation qui ne pourront alors se dérouler que sur autorisation du Président du Tribunal de Première Instance auquel il revient d'apprécier le motif ou l'absence de motif justifiant l'opposition.

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

UNE MISSION D'EXERCICE DES DROITS D'ACCÈS DES PERSONNES CONCERNÉES

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

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

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

Il concerne également les informations traitées par les organismes assujettis à la Loi n° 1.362 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, relatives aux obligations de vigilance, de déclaration et d'information auprès du Service d'Information et de Contrôle sur les Circuits Financiers.

DES SANCTIONS ADMINISTRATIVES

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

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

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

LE BUDGET DE LA COMMISSION

Pour l'année 2021 la Commission a bénéficié d'un budget total de 1.362.800,00 € se répartissant ainsi :

- 861.800,00 € au titre des crédits de fonctionnement, dont plus de la moitié est consacrée au paiement du loyer de ses locaux ;
- 501.000,00 € au titre de ses dépenses salariales, en diminution par rapport à l'année précédente.

Afin d'anticiper l'évolution de ses missions, la CCIN a demandé une modification de son organigramme dans le but de renforcer ses compétences. Cette modification devrait intervenir en début d'année 2023.

LE SECRÉTARIAT GÉNÉRAL DE LA COMMISSION

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

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

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

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

Il a notamment pour missions :

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

02

LE RÉPERTOIRE PUBLIC DES TRAITEMENTS

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

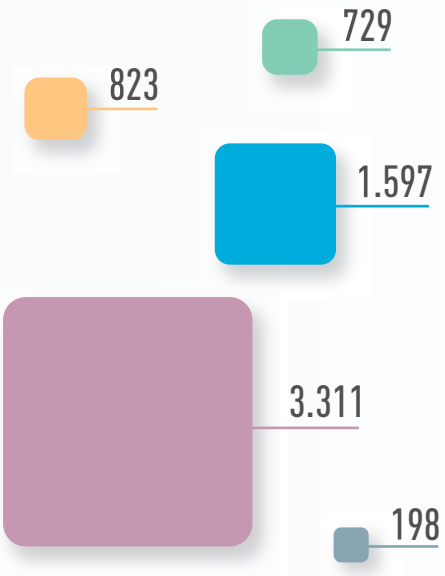
Il peut être consulté au siège de la Commission par toute personne physique ou morale souhaitant s'assurer de l'existence légale d'un traitement automatisé d'informations nominatives.

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

Nombre total de traitements inscrits au répertoire public au 31 décembre 2021

6.658 se répartissant ainsi :

- **729** traitements du secteur public ou assimilé
- **823** traitements ayant fait l'objet d'une autorisation de la Commission
- **1.597** traitements ayant fait l'objet d'une déclaration ordinaire
- **3.311** traitements ayant fait l'objet d'une déclaration simplifiée
- **198** 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
DS		26	26	68	21	16	45	46	19	54	856	144	86	180	201	162	221	243	326	188	177	206
DO	5	20	20	75	51	60	55	82	42	56	51	32	79	55	121	115	81	140	141	98	82	136
DA	6	22	22	13	17	11	2	12	16	4	22	38	71	68	67	23	34	38	54	35	66	88
DAUT								1		1	7	38	38	31	87	62	89	119	90	97	72	91
TRANSFERT														1	1	4	21	21	41	29	26	54

Nombre de nouveaux traitements inscrits au répertoire en 2021

575 traitements ont été inscrits au répertoire public, se répartissant comme suit :

Traitements ayant fait l'objet d'un avis favorable à leur mise en œuvre, relevant du secteur public ou assimilé	88
Traitements dont la mise en œuvre a été autorisée par la Commission	91
Traitements ayant fait l'objet d'une déclaration ordinaire	136
Traitements ayant fait l'objet d'une déclaration simplifiée	206
Autorisations de transfert de données vers un Pays ne disposant pas d'un niveau de protection adéquat	54

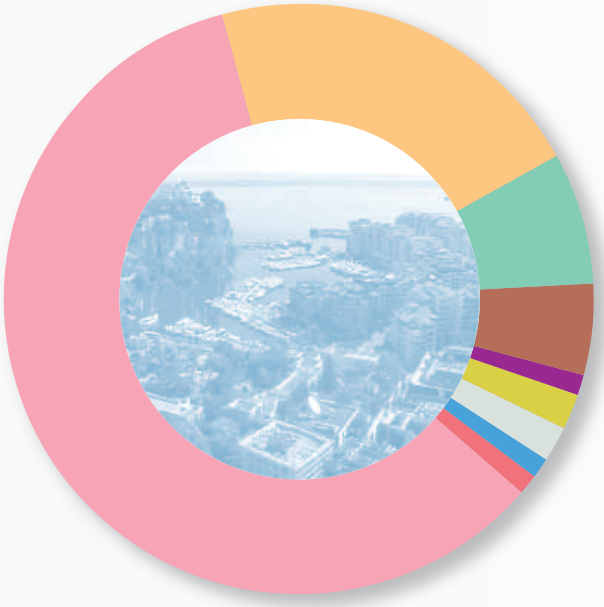
Nombre de délibérations rendues par la Commission en 2021

Au cours de l'année écoulée, la Commission a rendu
274 délibérations se répartissant ainsi :

11 autorisant la mise en œuvre ou la modification de traitements :

- **32** autorisations relatives à des dispositifs de vidéosurveillance
- **31** autorisations relatives aux traitements concernant plus spécifiquement le secteur bancaire et assimilé
- **10** autorisations relatives aux enregistrements téléphoniques
- **4** autorisations relatives à la messagerie électronique
- **10** autorisations relatives à des dispositifs de contrôle d'accès biométriques ou non
- **6** autorisation relative aux alertes professionnelles
- **3** autorisations relatives aux habilitations
- **9** autorisations relatives aux traitements exploités par les avocats
- **5** autorisations relatives aux traitements de contentieux
- **1** autorisation relative à un traitement de lutte contre le blanchiment de capitaux exploité par un établissement de jeux
- **1** refus d'autorisation concernant un traitement de pilotage du parc informatique et de l'optimisation de l'expérience utilisateur

99 portant avis favorable à la mise en œuvre ou à la modification de traitements :



- **59** demandes d'avis présentées par le Ministre d'Etat
- **21** demandes d'avis présentées par le CHPG
- **7** demandes d'avis présentées par la Mairie de Monaco
- **5** demandes d'avis présentées par Monaco Telecom
- **1** demande d'avis présentée par la SMEG
- **2** demandes d'avis présentées par l'Office de la Médecine du Travail
- **2** demandes d'avis présentées par la SMA
- **1** demande d'avis présentée par le Nouveau Musée National
- **1** demande d'avis présentée par le Conseil National

1 portant avis défavorable à la mise en œuvre d'un traitement

54 autorisant un transfert d'informations nominatives vers un Pays ne disposant pas d'un niveau de protection adéquat

7 portant avis sur des projets de textes transmis par le Ministre d'Etat

1 Portant sur une mission d'investigation

03

LE PROJET DE LOI RELATIVE À LA PROTECTION DES DONNÉES PERSONNELLES

En fin d'année 2020, par délibération n° 2020-151 du 4 novembre 2020, la Commission avait rendu un avis sur une première version du projet de Loi relative à la protection des données personnelles, élaboré dans le cadre d'un Groupe de Travail ad hoc entre ses Services et ceux du Gouvernement[1]. Toutefois ces travaux, qui avaient débuté en 2018, n'avaient pas permis à la Commission de faire entendre ses remarques sur de nombreux sujets.

Aussi au cours de l'année 2021 trois réunions ont eu lieu avec le Ministre d'Etat au cours desquelles la CCIN est revenue sur les principales problématiques liées à ce projet de Loi afin de tenter d'y remédier avant son dépôt au Conseil National. L'objectif de la refonte totale du droit interne en la matière est tout à la fois de se conformer à la Convention 108 du Conseil de l'Europe, telle que modifiée par son Protocole d'amendement, et d'intégrer les standards applicables sur le territoire de l'Union européenne résultant du Règlement Général sur la Protection des Données (RGPD) et de la Directive UE 2016/680 dite « *Directive Police Justice* ». Aussi les préoccupations principales de la Commission ont concerné les éléments du projet de Loi sur lesquels une attention particulière serait portée lors de l'examen, par la Commission européenne, du niveau de protection offert par la nouvelle législation monégasque en matière de protection des données personnelles.

La première réunion s'est tenue au début du mois de mai, et a permis à la délégation de la CCIN, conduite par son Président, d'aborder avec SEM le Ministre d'Etat, comme elle l'avait fait dans sa délibération n° 2020-151 portant avis sur ce projet de Loi, l'exclusion envisagée du champ de compétence de la future Autorité de Protection des Données Personnelles (APDP) de certains traitements mis en œuvre dans le cadre de la Loi n° 1.430 portant diverses mesures relatives à la préservation de la sécurité nationale. Elle a une nouvelle fois souligné que le Référentiel d'adéquation à l'aune duquel la Commission européenne examine les demandes d'adéquation consacre un chapitre entier aux « *Garanties essentielles dans les pays tiers en matière d'application des lois et d'accès pour des raisons de sécurité nationale afin de limiter les ingérences dans les droits fondamentaux* ». Aussi la CCIN a une nouvelle fois indiqué que si cette exclusion devait être maintenue, il importerait alors que la Commission, qui aura la charge du contrôle des traitements y afférents, bénéficie de la totalité des attributs d'une Autorité Administrative Indépendante, et des moyens pour accomplir pleinement ses missions de contrôle.

La CCIN a également rappelé la nécessité de se conformer aux standards européens en matière de transparence, et de ce fait de pouvoir rendre davantage accessibles les avis qui seront rendus par la future APDP appelée à succéder à la CCIN.

Faisant suite à cette première réunion, SEM le Ministre d'Etat s'est rendu dans les locaux de la Commission le 29 juillet 2021 afin d'évoquer les points principaux soulevés par la CCIN dans l'optique de l'obtention d'une décision d'adéquation. La Commission a alors été informée qu'une récente réunion s'était tenue avec le Président du Conseil d'Etat, dont l'avis sur le projet de Loi avait également été sollicité. Elle a pris acte des déclarations

[1] Voir Rapport d'activité 2020 p 71 et suivantes

du Ministre d'Etat selon lesquelles le Gouvernement n'envisageait pas de revoir sa position concernant l'exclusion du champ de compétence de l'APDP des traitements de sécurité nationale. En revanche il a été annoncé qu'une amélioration serait faite en matière de transparence, afin d'étendre la possibilité de publier les avis de l'APDP. Il était enfin annoncé que des arbitrages finaux devaient être faits à l'automne, pour un dépôt du projet de Loi au Conseil National avant la fin de l'année 2021

En date du 10 novembre 2021 le Ministre d'Etat a adressé à la Commission une nouvelle version du projet de Loi, laquelle comportait au principal 9 nouveaux articles dont l'objectif était de davantage

Visite de SEM Pierre DARTOUT dans les locaux de la CCIN le 29 juillet 2022

prendre en compte certains souhaits de la CCIN concernant la protection des données des personnes décédées, l'encadrement des transferts d'informations, ainsi que les traitements de sécurité nationale.

UN SECOND AVIS SUR LE PROJET DE LOI RELATIVE À LA PROTECTION DES DONNÉES PERSONNELLES

Dans un délai une nouvelle fois très contraint la Commission a rendu, par délibération n° 2021-260 du 1er décembre 2021, un avis sur ces projets d'articles mais également sur l'ensemble des nombreuses modifications apportées au projet de Loi depuis sa précédente saisine en 2020.

Elle est revenue sur le maintien des choix gouvernementaux en matière de contrôle des traitements dits de sécurité nationale, et sur les conséquences qu'il y a lieu d'en tirer dans la perspective de l'obtention d'une décision d'adéquation, en suspens depuis 2012.

Elle s'est par ailleurs prononcée sur les différentes modifications apportées au projet de Loi depuis sa saisine initiale, et dont certaines étaient porteuses de problématiques nouvelles.

Enfin, la Commission a relevé les différents points qu'elle avait soulevés et qui n'ont pas, totalement ou partiellement, été pris en compte dans la nouvelle version du projet de Loi.

Le maintien des dispositions en matière de sécurité nationale

La Commission a de nouveau insisté sur la nécessité de respecter le référentiel d'adéquation établi par le Comité européen à la protection des données (CEPD ex. Groupe 29) pour l'obtention d'une décision d'adéquation, étant précisé qu'en matière de sécurité nationale ledit référentiel mentionne que :

- le traitement devrait reposer sur des règles claires, précises et accessibles (base juridique) ;
- la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis doivent être démontrées ;
- le traitement doit faire l'objet d'un contrôle indépendant ;
- les particuliers doivent disposer de voies de recours effectives.

Lors de son avis initial rendu en 2020, la CCIN avait déjà insisté sur le fait que la Commission instituée par l'article 16 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale (« *Commission Article 16* ») contrôlait l'opportunité du recours à des techniques de renseignement, mais non la mise en œuvre des traitements de données personnelles en découlant, ou le respect des droits associés, tel que le droit d'accès indirect.

Au cours de l'examen de la nouvelle version du projet de Loi, la CCIN a pourtant constaté l'introduction, au sein du dispositif, d'une section intitulée « *Traitements mis en œuvre dans le cadre des dispositions des articles 9 à 15 et 18 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale* » et d'un article précisant que la Commission instituée à l'article 16 de la Loi n° 1.430 serait également chargée de contrôler, en toute indépendance, les traitements mis en œuvre dans le cadre des articles 9 à 15 et 18 de ladite Loi, conformément à ses dispositions, ainsi qu'à celles de la Loi en matière de protection des données applicables à ces traitements.

La CCIN a une fois de plus souligné qu'aucun traitement n'est mis en œuvre dans le cadre de ces articles, puisque les articles 9 à 15 de la Loi n° 1.430 permettent le recours à des techniques de renseignement par lesquelles s'opèrent certaines collectes de données, sans toutefois consacrer de traitements de données, et l'article 18 instaure pour sa part un secret de sécurité nationale, sans pour autant emporter de création de fichiers, secret qui concerne également les entités privées ayant qualité d'Organisme d'Importance Vitale (OIV).

Concernant le contrôle qui devra être effectué sur les traitements dits de sécurité nationale, et qui relèverait du champ de compétence de la « *Commission article 16* », la CCIN a souligné que le projet de Loi ne prévoyait aucune disposition sur ce point, alors même que les standards internationaux imposent un contrôle effectif, et l'existence de moyens nécessaires pour sa réalisation. Aussi la CCIN a renouvelé ses remarques appelant à une véritable réforme de la Loi n° 1.430 en insistant sur le fait que le rajout d'une nouvelle section au sein du dispositif du nouveau projet de Loi n'était pas de

nature à doter la « *Commission Article 16* » d'une réelle indépendance fonctionnelle et de pouvoirs de contrôle clairement définis.

Enfin, elle est revenue sur la problématique résultant du maintien dans le nouveau projet de Loi de l'opposabilité du secret de sécurité nationale aux agents investigateurs de l'APDP, en illustrant son propos d'exemples concrets ayant vocation à alerter, à nouveau, les Services gouvernementaux sur la portée pratique de cette opposabilité, dans des domaines pourtant sans lien avec la préservation de la sécurité nationale.

Les modifications apportées au projet de Loi depuis la précédente saisine de la CCIN

Plusieurs modifications ont été apportées au projet de Loi dont la Commission avait été saisie en 2020. Si elle a salué l'introduction d'éléments de nature à renforcer les droits des personnes (introduction d'un article sur les données relatives aux personnes décédées) ainsi que la prise en compte de certaines de ses remarques, elle a également constaté l'ajout de nouvelles dispositions problématiques, qui ont été rectifiées suite à ses commentaires.

La Commission a, par ailleurs, regretté le maintien de l'exclusion des « *mesures à caractère social* » de la catégorie des données sensibles et a considéré que des précisions sur la notion de « *personnes vulnérables* », introduite dans le projet de Loi, devraient être apportées afin d'en définir les contours.

La Commission s'est également interrogée sur l'exclusion d'office du Délégué à la Protection des Données (DPO) concernant l'accès à certaines données et opérations relatives à des traitements particulièrement sensibles dans la mesure où, compte tenu de ses missions, il devrait pouvoir accéder à l'intégralité des systèmes d'informations et des données traitées. Aussi, elle a suggéré, en lieu et place d'une exclusion d'office, de prévoir la rédaction de lettres de missions destinées aux DPO, afin de détailler précisément le périmètre de leurs missions.

Concernant la composition de la future APDP appelée à lui succéder, laquelle devrait comprendre 4 magistrats (2 titulaires et 2 suppléants), la Commission a suggéré, pour éviter d'éventuelles difficultés de candidatures, qu'il soit possible qu'un magistrat ayant déjà effectué deux mandats puisse à nouveau être nommé, à l'issue d'un délai de vacuité à préciser.

S'agissant des traitements dits de « *Police Justice* », La Commission a regretté qu'il soit désormais envisagé que le magistrat nommé sur proposition du Président de la Cour de Révision effectue, qui plus est seul, les opérations de contrôle de ces traitements. D'une part, la Commission ne comprend

pas pourquoi certains traitements devraient bénéficier de dispositions dérogatoires en matière de contrôles. D'autre part, cela conduirait à ce qu'un magistrat ayant participé à la décision d'effectuer un contrôle l'effectue lui-même, ce qu'elle souhaite éviter.

La Commission a par ailleurs remarqué l'introduction de nouvelles incompatibilités concernant les Membres de l'APDP. Si elle a souligné qu'elle comprenait l'incompatibilité avec la qualité de Membre de la Commission Supérieure des Comptes, tel n'est pas le cas pour celle de Membre titulaire ou suppléant d'un organisme consultatif de l'Etat. Elle a ainsi regretté l'introduction d'une notion aux contours flous, eu égard d'une part, aux spécificités de la Principauté qui compte un nombre plus limité de personnes ayant une connaissance spécifique du Pays et d'autre part, à l'absence de liste exhaustive des organismes consultatifs de l'Etat. Afin de prévenir toute insécurité juridique, elle a recommandé la suppression de ce terme, qui renvoie à des organismes non clairement identifiés ainsi que la rédaction d'une liste identifiant de manière exhaustive les organismes concernés par l'incompatibilité.

Au sujet de la coopération et de l'assistance mutuelle avec des Autorités de protection étrangères, la Commission avait été étonnée de constater qu'en cas de refus de coopération d'une de ces Autorités, une sanction puisse être prononcée à l'encontre d'un responsable de traitement ou d'un sous-traitant, situé à Monaco.

Outre le maintien de l'opposabilité du secret de sécurité nationale, la Commission a noté que le secret défini à l'article 308-1 du Code pénal pourrait désormais être également opposé à ses membres, agents ou investigateurs lors d'opérations de contrôle et l'a regretté d'autant plus que le périmètre attaché y est potentiellement extrêmement large. Elle a estimé qu'il aurait été, a minima, souhaitable et davantage ambitieux d'encadrer l'accès aux documents administratifs notamment par les administrés et de définir, en droit interne, les conditions dans lesquelles le droit d'accès pourrait être restreint ou reporté. De même, elle a réitéré ses regrets de ne pas avoir été saisie, en amont, de l'Ordonnance Souveraine relative aux archives d'intérêt public en dépit de son lien incontestable avec la protection des informations nominatives.

La Commission a également déploré l'existence d'une incompréhension de la part des Services gouvernementaux venant limiter artificiellement les pouvoirs de sanction de la future APDP en la contraignant presque, quelle que soit la gravité d'un manquement constaté, a d'abord mettre en demeure un responsable de traitement en défaut avant de pouvoir le sanctionner.

De même, elle a constaté l'existence de nombreuses modifications apportées aux articles relatifs aux transferts de données liés aux traitements dits de « Police-Justice » et de sécurité nationale, ainsi qu'au chapitre relatif aux transferts de droit commun. Il était ainsi prévu que les premiers puissent s'effectuer, vers un Etat ou une organisation internationale n'assurant pas un niveau de protection adéquat, sous réserve du respect d'un engagement exécutoire dans la Principauté ; de l'analyse des circonstances du transfert ; de l'existence de garanties appropriées. Outre le fait qu'il est impossible de savoir s'il s'agit, ou non, de conditions cumulatives, la Commission a rappelé que la Directive européenne « *Police-Justice* », dont s'inspire également le projet de Loi, exige que l'engagement exécutoire dispose en son sein de garanties appropriées, ce que ne prévoit pas le dispositif monégasque en projet. Aussi, elle a estimé qu'il serait préférable que l'exposé des

motifs précise que les garanties appropriées ne s'analysent pas en un simple renvoi à celles énoncées à l'article régissant, de manière exclusive, les transferts de droit commun.

Concernant ces derniers, elle s'est étonnée qu'ils puissent être effectués vers un pays ne disposant pas d'un niveau de protection adéquat, sur la base de règles d'entreprises contraignantes approuvées par une Autorité d'un pays tiers, sans validation préalable de la future APDP. Ces transferts pourraient, de plus, être justifiés par le respect d'un engagement international exécutoire dans la Principauté, alors que cela est expressément limité aux traitements découlant de la Directive européenne « Police Justice ». La Commission a enfin acté que la liste des pays disposant d'un niveau de protection adéquat/approprié serait désormais établie par voie d'Arrêté Ministériel. Elle a rappelé que seuls devaient y figurer les pays disposant d'une législation en matière de protection des données offrant aux personnes concernées de la Principauté une protection adéquate effective. Elle a à cet égard suggéré qu'il lui soit possible d'alerter le Gouvernement sur des pratiques/législations qui ne permettraient plus à un Etat d'être mentionné sur cette liste.

Concernant enfin l'information des personnes concernées, contrairement à ce que prévoit le projet de Loi, la Commission a insisté sur l'impossibilité qu'un responsable de traitement puisse satisfaire à cette obligation en effectuant une information collective économiquement intéressante pour lui, et a rappelé que la personne concernée doit pouvoir être valablement informée par le responsable de traitement au moment de la collecte de ses données.

Les points non adressés ou partiellement pris en compte

La Commission a par ailleurs regretté que certains points sur lesquels elle avait insisté tout au long des travaux préparatoires n'aient finalement pas été pris en compte dans le cadre de la nouvelle version du projet de Loi.

Tel est notamment le cas de l'absence de formalisme spécifique en matière de traitement de données de santé. En effet, il lui avait été objecté que ceci serait pris en compte dans le cadre d'un projet de Loi spécifique consacré aux dites données, projet de Loi dont elle n'a à ce jour aucune visibilité concernant son élaboration.

S'agissant des analyses d'impact la CCIN a une nouvelle fois déploré que le Gouvernement soustrait à toute formalité les mesures de surveillance constante sur le lieu de travail, d'autant qu'il existe à l'égard des salariés un risque fort de pratiques intrusives et disproportionnées.

En outre, elle s'est questionnée sur la pertinence de laisser à l'exécutif le soin de définir lui-même la liste des critères permettant de déterminer si un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés, le RGPD prévoyant pour sa part que cette liste soit établie par les Autorités de protection.

Elle s'est par ailleurs inquiétée de ce que le dispositif prévoyait la mise à disposition, en temps réel, au bénéfice de la Direction de la Sûreté Publique (DSP), des images des dispositifs de vidéosurveillance installés dans des parties privatives. Ceci a conduit la Commission à alerter les rédacteurs du projet de Loi sur la proportionnalité d'une telle mesure, qui plus est en l'absence d'encadrements précis.

LES ULTIMES MODIFICATIONS DU PROJET DE LOI AVANT SON DÉPÔT AU CONSEIL NATIONAL

Compte tenu des nombreux points soulevés dans sa délibération n° 2021-260 du 1er décembre 2021 portant avis sur la nouvelle version du projet de Loi relative à la protection des données personnelles, dont certains revêtent une acuité toute particulière, la Commission a souhaité que son Président rencontre à nouveau SEM le Ministre d'Etat afin de l'alerter sur des sujets majeurs qui nécessiteraient d'être revus avant que le projet de Loi ne soit déposé au Conseil National. C'est dans ce cadre qu'une nouvelle réunion a été organisée avec le Ministre d'Etat le 10 décembre 2021. Les échanges ont bien évidemment concerné au principal les traitements de données en matière de préservation de la sécurité nationale, pour lesquels les standards européens à l'aune desquels l'adéquation de la Principauté sera examinée requièrent un contrôle effectif et indépendant.

Cette réunion a utilement permis que certaines dispositions problématiques soient modifiées, dont notamment les incompatibilités des futurs membres de l'APDP, le retrait de la possibilité pour la Direction de la Sûreté Publique (DSP) de se connecter à des images de vidéosurveillance dans des lieux privatifs et de l'opposabilité du secret tel que prévu à l'article 308-1 du Code pénal. De plus, est apparu un aménagement textuel permettant l'accès à des zones protégées par le secret de sécurité nationale, lors d'un contrôle portant sur un traitement relevant de la compétence de l'APDP. Le Ministre d'Etat a également annoncé la prise en compte des souhaits de la CCIN concernant les mesures préalables aux sanctions, qui hélas ne s'est pas concrétisée dans la version du projet de Loi déposée au Conseil National.

Si la Commission a relevé que les modifications apportées suite à la réunion avec SEM le Ministre d'Etat contribuent à certains égards au renforcement de la protection des données personnelles et démontrent une certaine volonté gouvernementale de prendre en compte ses remarques, elle a toutefois souligné que les dispositions en lien avec la préservation de la sécurité nationale n'avaient subi que de faibles aménagements, et que de nombreuses observations qu'elle avait formulées n'ont pas été prises en compte dans le projet de Loi tel qu'il a été déposé au Conseil National en fin d'année 2021.

A la lecture de ce projet, accessible sur le site Internet du Conseil National[2], la Commission a constaté que certains éléments sur lesquels elle avait pourtant obtenu un accord, n'étaient pas pris en compte dans cette dernière version du projet de Loi. Aussi en 2022 la CCIN s'attachera à obtenir les modifications souhaitées, et acceptées en son temps par le Gouvernement.

[2] https://www.conseil-national.mc/2021/12/27/n-1054-projet-de-loi-relative-a-la-protection-des-donnees-personnelles/

04

LA CCIN ET LES DROITS DES PERSONNES CONCERNÉES

LES CONSULTATIONS DU RÉPERTOIRE PUBLIC DES TRAITEMENTS

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

Les informations figurant dans ledit répertoire sont les suivantes :

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

Au cours de l'année 2021 ce répertoire a été consulté 5 fois :

- 4 fois par des sociétés, ou par des Cabinets de conseil pour le compte de leurs clients afin de faire le point sur les traitements qui ont déjà fait l'objet de formalités préalables, dans la perspective de poursuivre, ou d'initier, la mise en conformité ;
- 1 fois par une salariée dont l'employeur a fait installer des caméras sur le lieu de travail. Constatant que ce dispositif de vidéosurveillance n'avait fait l'objet d'aucune autorisation de mise en œuvre de la part de la CCIN, la salariée a déposé une plainte auprès d'elle.

LES PLAINTES

28 plaintes ont été adressées à la Commission en 2021, en forte augmentation par rapport à l'année précédente au cours de laquelle elle avait été saisie par 19 personnes.

Du bon usage des données personnelles

L'article 16 de la Loi n° 1.165 confère à toute personne le droit d'exiger que les informations nominatives la concernant soient rectifiées, complétées, clarifiées, mises à jour ou supprimées lorsqu'elles se sont révélées inexactes, incomplètes, équivoques ou périmées.

Le droit de suppression

14 plaintes portant sur le droit de suppression de contenus en ligne ont été déposées auprès de la CCIN en 2021. Sur ces 14 plaintes, 3 ont été jugées irrecevables, faute d'éléments nécessaires pour les traiter, et 3 ont été résolues directement par les plaignants auprès des médias concernés avant même que la CCIN ait eu à intervenir.

Très souvent les piratages de comptes Facebook et Instagram peuvent être résolus très facilement par les particuliers eux-mêmes en suivant tout simplement les procédures mises en place par les réseaux sociaux. Aussi, la Commission encourage les plaignants à contacter dans un premier temps lesdits réseaux avant de la saisir uniquement en cas de démarches infructueuses. Un petit guide des procédures de réinitialisation du mot de passe ou de récupération de compte figure dans la section « Fiches Pratiques » de ce rapport ainsi que sur le Site Internet de la CCIN.

Sur les 8 demandes finalement traitées, 6 ont concerné les réseaux sociaux.

- La première de ces demandes avait pour objet 5 faux comptes (2 sur Facebook, 1 sur Instagram, 1 sur LinkedIn et 1 sur Twitter) créés au nom d'une haute personnalité de la Principauté. Ces faux comptes étaient entre autres utilisés pour poster des commentaires sur d'autres pages officielles, ce qui portait non seulement atteinte à cette personnalité mais induisait également les résidents monégasques en erreur puisque pensant que ces comptes constituaient un média officiel, ils étaient de plus en plus nombreux à s'y abonner.

- Une autre plainte a porté sur la suppression de deux comptes Instagram qui, suite à un piratage, étaient utilisés pour envoyer des photos de mineurs à connotation sexuelle.

- La CCIN a également été saisie d'une demande de suppression d'un faux compte LinkedIn qui usurpait là encore l'identité d'une très haute personnalité à des fins d'escroquerie.

- Une demande de récupération d'un compte Facebook et d'un compte Instagram qui avaient été piratés, a par ailleurs été effectuée au nom d'une athlète monégasque. Celle-ci, connue publiquement, avait entamé la procédure de certification de son compte Instagram par le biais de l'application officielle du réseau social sur son téléphone. En réponse à sa demande, elle avait toutefois été invitée à communiquer une copie de sa pièce d'identité et à modifier l'adresse email associée à son compte, ce qu'elle a malheureusement fait. En effet, suite à ces deux actions, les pirates ont pu prendre le contrôle de ce compte ainsi que de celui de Facebook qui lui était associé.

- Enfin, deux institutions monégasques ont demandé l'aide de la CCIN pour récupérer leurs comptes officiels respectifs qui n'étaient plus accessibles.

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

Les deux autres plaintes reçues en 2021 avaient pour objet de faux sites internet.

- Dans le premier cas, un faux site Internet avait été créé sur Wix au nom d'une étudiante afin de poster du contenu à caractère sexuel. Si cette jeune personne n'apparaissait pas sur les images et vidéos postées, sa photo était toutefois utilisée en icône de profil et en page de couverture.

Une fois saisie, la CCIN a obtenu la suppression de ce site en moins de 24 heures.

- La deuxième plainte concernait deux faux sites Internet créés sur Google, chacun au nom de deux personnes différentes, afin de colporter des accusations injustifiées à leur encontre. Le moteur de recherche a donné une suite favorable à la première demande de déréférencement car, même si le site faisait référence au rôle professionnel de la personne concernée, Google a considéré que la plaignante n'était pas une personne publique et que d'autres éléments de sa vie privée étaient présents sur l'URL.

Le moteur de recherche a refusé en revanche de déréférencer le second site, estimant ne pas être en mesure de se prononcer sur l'exactitude des déclarations faites à l'encontre du plaignant, d'autant plus que d'autres éditeurs, notamment le Consortium international des journalistes d'investigation, avaient fait des rapports sur des questions connexes le concernant.

En cas de diffamation présumée, la procédure judiciaire est le meilleur moyen pour résoudre les questions relatives à l'exactitude des déclarations en question, plutôt qu'une procédure en vertu de la Loi sur la protection des données contre un fournisseur de moteurs de recherche qui n'a pas participé au reportage ou à la publication en question.
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

Le droit d'accès

Conformément à l'article 13 de la Loi n° 1.165 toute personne physique a le droit d'accéder aux informations la concernant et d'obtenir qu'elles soient modifiées s'il y a lieu, l'article 15 venant pour sa part préciser que la réponse à une demande d'accès doit s'effectuer sous un délai d'un mois.

Saisie sur le fondement de ce droit d'accès, la Commission a eu à connaître de deux plaintes.

Dans le premier dossier, il s'agissant d'une personne inscrite dans une agence d'intérim, laquelle n'avait donné aucune suite à sa demande de communication des noms des entités auxquelles sa candidature avait été transmise. Sur ce point, le Code de déontologie des entreprises de prestations de services et de personnel intérimaire précise que ces entreprises ont le statut d'employeur des personnes qui bénéficient de leurs services, et donc à ce titre elles ont les mêmes obligations. En l'espèce la société d'intérim ne voulait pas communiquer les informations sous le prétexte que les entités destinataires des éléments souhaitaient garder cette information confidentielle, dans un secteur d'activité concurrentiel. L'intervention de la CCIN a permis que le plaignant obtienne très rapidement les informations souhaitées.

Le second cas a concerné des enregistrements téléphoniques pour lesquels un ancien salarié a fait valoir son droit d'accès, dans un contexte de conflit avec sa hiérarchie. La CCIN a alors rappelé au responsable de traitement les bonnes pratiques en la matière, en l'invitant à procéder à une retranscription des enregistrements téléphoniques souhaités tout en préservant les droits des tiers dont l'identité serait inconnue du demandeur. Il a également été précisé que le responsable de traitement pouvait faire procéder à cette retranscription par un huissier de justice s'il le souhaitait, et que les données pouvaient être transmises au conseil du demandeur, dûment mandaté à cet effet.

L'octroi de délais de réponse à une demande de droit d'accès

La législation prévoit que le délai légal de réponse à une demande de droit d'accès est d'un mois. Toutefois le Président de la CCIN peut, après avis favorable de la Commission, accorder des délais de réponses supplémentaires.

Saisie d'une telle demande, la CCIN a précisé les conditions devant encadrer l'octroi de délais :

- *les motifs invoqués à l'appui de la demande doivent être suffisamment étayés, afin de permettre à la Commission d'en apprécier le bienfondé ;*
- *le délai supplémentaire souhaité doit être précisé, là aussi pour que la Commission puisse s'assurer qu'il est en adéquation avec les justifications invoquées par le responsable de traitement.*

En l'espèce le responsable de traitement a mis en avant la très grande quantité de documents concernés par le droit d'accès du demandeur (800 environ), qui devaient faire préalablement l'objet d'un tri minutieux afin de respecter les droits des tiers.

Prenant en considération ces éléments, la Commission a accordé le délai de 3 mois supplémentaires, sollicité par le responsable de traitement.

La prospection commerciale

Deux personnes ont saisi la CCIN après avoir reçu des emails et des sms publicitaires, émanant d'entités qu'elles ne connaissaient pas.

Les règles relatives à la prospection commerciale ont été rappelées aux entités expéditrices de ces messages, et les personnes ont été informées de leur possibilité de se désinscrire des listes de diffusion. A cet égard la CCIN a invité des entités à rendre plus visibles et accessibles les liens permettant de procéder à ce désabonnement.

Les messages de démarchage publicitaires concernaient ici des marques commerciales, inconnues des plaignants, mais commercialisées par des enseignes dont ils étaient clients.

La législation en matière de prospection commerciale :

Loi n° 1.383 du 2 août 2011, modifiée, pour une Principauté numérique

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

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

Dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le consommateur puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé.

La messagerie électronique professionnelle

La CCIN a une nouvelle fois été saisie par un ancien salarié qui a constaté que plusieurs mois après son départ son adresse email nominative était encore active, ce qui permettait à son ancien employeur de répondre à des messages qu'il avait reçus, et, pire encore, de prendre connaissance de messages d'ordre privé adressés sur sa messagerie professionnelle.

Là encore la CCIN est intervenue afin que l'adresse email nominative de l'ancien salarié soit désactivée immédiatement.

Cette problématique étant récurrente la CCIN a rédigé une Fiche pratique dédiée à la messagerie électronique professionnelle[3] et mis en ligne un rappel des bonnes pratiques sur son site Internet.

L'accès aux données privées des salariés

Dans cette affaire le plaignant s'est aperçu que son ancien employeur avait accédé à sa boite email personnelle, depuis son ancien ordinateur professionnel, et que non seulement il ne s'était pas immédiatement déconnecté, mais qu'il avait copié certains messages et les avait transmis à des tiers.

Face à la gravité de cette atteinte à la vie privée la CCIN a immédiatement saisi le Procureur Général.

L'exploitation des traitements automatisés d'informations nominatives

La vidéosurveillance

7 plaintes au total ont concerné des dispositifs de vidéosurveillance exploités par des entités privées, dont 2 dans des immeubles d'habitation.

Dans ces 2 cas la CCIN a fait réorienter les caméras afin qu'elles ne filment pas le domaine public, et notamment les voies circulation ainsi que les trottoirs alentours.

[3] Voir à la fin du présent Rapport d'activité.

Dans l'une de ces 2 affaires elle a fait implémenter un dispositif de mise en veille de l'écran de visualisation dans la loge du concierge, ainsi qu'un système d'habilitation d'accès permettant d'historiser les données de connexions aux images.

4 autres plaintes ont émané de salariés, ou d'organisations syndicales, concernant une utilisation des caméras pour surveiller le travail des employés :

- dans 2 affaires les caméras, qui n'avaient fait l'objet d'aucune formalité, ont été désactivées immédiatement dans l'attente des obtentions des autorisations d'exploitation délivrées respectivement par SEM le Ministre d'Etat et par la CCIN ;

- dans la 3ème affaire le dispositif a été régularisé dans de très brefs délais, et les caméras qui étaient implantées au-dessus des postes de travail des gardiens, les soumettant à une surveillance constante et inopportune, ont été réorientées dès l'intervention de la CCIN ;

- la 4ème affaire a concerné un dispositif de vidéosurveillance autorisé par la CCIN mais dont les images seraient utilisées pour surveiller le travail et le temps de travail des salariés, ce que la Commission interdit. Par ailleurs, 2 caméras supplémentaires avaient été implantées, et les habilitations d'accès aux images étendues par rapport au périmètre de l'autorisation initiale. Lors de la régularisation de ces modifications la CCIN a demandé que les personnes ayant accès aux images, et notamment les supérieurs hiérarchiques, soient explicitement informées que les images ne peuvent en aucun cas être utilisées à d'autres fins que la préservation de la sécurité des personnes et des biens.

1 plainte a émané d'un client qui a constaté que des caméras avaient été installées sans aucune mention d'information à l'attention des personnes qui fréquentent ce commerce (aucun pictogramme à l'entrée). Les caméras ont été désactivées suite à l'intervention de la CCIN.

Le dispositif de gestion des courses de taxis

La Commission a une nouvelle fois eu à connaître de problématiques liées à l'exploitation du dispositif de gestion des courses de taxis, et dont les données ont été communiquées, de manière illégitime, à l'Association professionnelle des conducteurs de taxis. Dans ce cadre un conducteur de taxi a été convoqué par la Section des taxis de la Direction de la Sûreté Publique. Lors des échanges intervenus avec les membres de ladite section la CCIN a précisé que l'Association des conducteurs de taxis n'a en charge que la gestion technique du dispositif, et que cette mission ne lui permet pas d'avoir accès aux données identifiantes des membres de la profession. De plus une réunion a eu lieu avec les représentants de cette Association et le Service de l'Etat en charge des taxis afin de rappeler les bonnes pratiques.

Par ailleurs en 2021 la CCIN a été interrogée à de nombreuses reprises par des personnes qui, sans souhaiter la saisir formellement de plaintes, désiraient connaître les règles applicables à tel ou tel domaine, afin de connaître leurs droits ou de faire respecter les bonnes pratiques.

Ceci a concerné des domaines aussi variés que :

- *l'envoi des certificats médicaux en cas d'arrêt de travail : un employeur avait mis en place une procédure demandant à ses salariés de lui adresser les certificats médicaux. La CCIN a immédiatement pris l'attache de cette entité et lui a demandé d'indiquer aux salariés qu'il leur appartient d'adresser directement à l'assureur ces certificats médicaux, aux fins de versement des compléments de salaires. Toutefois si par facilité les employés préfèrent les adresser à leur employeur, charge à lui d'en assurer la communication à l'assureur, ceci doit être fait sous pli cacheté et confidentiel, avec une interdiction formelle pour l'employeur de prendre connaissance du contenu du pli. La procédure a été modifiée sur le champ.*

- *l'obligation faite par des employeurs d'activer en permanence la web cam des salariés en télétravail, ou même au bureau : la CCIN a communiqué aux salariés qui l'ont contactée ce qui est permis ou non en la matière :*

  > *les web cam ne doivent pas être activées en permanence mais uniquement dans des circonstances spécifiques (participation à certaines réunions de travail par visioconférence par exemple). Cependant <u>les salariés doivent pourvoir refuser d'utiliser la caméra, sauf justification étayée le nécessitant</u> (tel pourrait être le cas par exemple lorsque la nature de la réunion justifie un moyen d'identification spécifique des participants). Dans le cas contraire le recours à la conférence téléphonique constitue une modalité adéquate de participation aux réunions de travail, que ces réunions se fassent en télétravail ou au bureau ;*

  > *les visioconférences ou les conférences téléphoniques ne doivent pas donner lieu à enregistrements, sauf justification particulière à des fins probatoires par exemple. Si tel est le cas les participants doivent en être préalablement informés, et ceci doit être préalablement déclaré à la CCIN.*

- *contactée au sujet de l'utilisation de caméras sur le lieu de travail, la CCIN a précisé les obligations des employeurs et les droits des salariés :*

  > *tout dispositif de vidéosurveillance mis en œuvre dans un lieu de travail est soumis à autorisation préalable du Ministre d'Etat et de la CCIN. Un tel dispositif ne doit être utilisé qu'à des fins de sécurité des personnes et des biens et ne doit en aucun cas servir à surveiller le travail ou le temps de travail des salariés. Les caméras ne doivent pas être orientées vers les postes de travail des salariés, sauf quelques cas très spécifiques (manipulation d'argent ou d'objets précieux par exemple) ;*

  > *les salariés doivent être préalablement informés de l'installation de caméras, par exemple par un pictogramme visuel situé aux entrées de l'établissement ;*

  > *comme pour tout traitement d'informations mis en œuvre par l'employeur les salariés disposent d'un droit d'accès aux images les concernant. Si le salarié le souhaite l'employeur doit lui remettre une copie des images sur lesquelles le salarié apparait, tout en préservant les droits des tiers ;*

  > *si un salarié estime qu'un dispositif n'est pas conforme il peut saisir la CCIN qui interviendra auprès du responsable de l'établissement, sans divulguer le nom de la personne qui l'a saisie sauf accord de sa part.*

LES INVESTIGATIONS

Un contrôle du dispositif de vidéosurveillance dans un immeuble d'habitation

La Commission a souhaité procéder à un contrôle concernant un dispositif de vidéosurveillance au sein d'un immeuble d'habitation qui avait reçu une autorisation de mise en œuvre quelques années auparavant, et ce afin de vérifier si les termes de son autorisation étaient respectés.

Comme elle le fait usuellement la Commission pose systématiquement des conditions aux autorisations qu'elle délivre, afin notamment de préserver la vie privée des résidents.

Parmi ces conditions figurent :

- l'interdiction de filmer les couloirs d'accès aux appartements ;
- l'interdiction de filmer l'intérieur des ascenseurs ;
- lorsque des écrans de visualisation des images au fil de l'eau sont situés dans les banques d'accueil des immeubles : obligation que ces écrans ne soient pas visibles par des personnes non habilitées ;
- implémentation d'une journalisation nominative des accès aux enregistrements ; ...

Ce contrôle n'ayant pas eu lieu suite à la réception d'une plainte, il s'est déroulé sur le fondement de l'article 18-1 de la Loi n° 1.165, avec la possibilité pour le responsable de traitement de s'y opposer, ce qu'il n'a pas souhaité faire.

Lors de ce contrôle il a été constaté que des filtres ou des caches occultent les couloirs d'accès aux appartements, ainsi que les portions de voie publique près des entrées de l'immeuble.

De même, aucune caméra ne filme les postes de travail des gardiens de l'immeuble, et les images ne sont pas conservées plus de 30 jours.

Les postes de visionnages des images mis à disposition des gardiens de l'immeuble sont mis en veille automatiquement après un temps d'inactivité, et les écrans sont situés à l'abri des regards des personnes non habilitées à les visionner.

Aussi, il a été relevé lors de ce contrôle que les termes de l'autorisation de mise en œuvre délivrée par la CCIN étaient respectés, mis à part sur un point : les caméras situées dans les ascenseurs filment l'intégralité des cabines, et pas uniquement les portes des ascenseurs.

Pour justifier cela il a été indiqué aux Agents contrôleurs que ces caméras répondaient à une demande des Sapeurs-Pompiers, l'immeuble étant en effet qualifié d'Immeuble de Grande Hauteur. Aussi en cas d'incendie les pompiers utiliseraient les caméras afin de s'assurer que les ascenseurs sont inoccupés.

Même si elle a émis des réserves sur le bienfondé de cette justification avancée par le syndic de l'immeuble, la Commission a souhaité que ce point fasse l'objet d'un échange avec les Pompiers, dans la mesure où elle ne voudrait pas que ses demandes gênent leurs interventions en cas d'incident de grande ampleur.

LES DEMANDES D'EXERCICE D'UN DROIT D'ACCÈS INDIRECT

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

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

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

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

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

Par ailleurs, depuis les modifications législatives intervenues en 2018, l'accès aux informations traitées à des fins de lutte contre le blanchiment de capitaux ne peut s'effectuer que par la CCIN, auprès des entités assujetties à la Loi n° 1.362 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption.

C'est dans ce cadre qu'au cours de l'année 2021 il a été procédé à l'exercice de 3 droits d'accès indirects auprès d'établissements bancaires et assimilés.

LES DÉCISIONS DE JUSTICE EN MATIÈRE DE PROTECTION DES INFORMATIONS NOMINATIVES

En 2021 le Tribunal Correctionnel a eu à se prononcer à deux reprises sur des affaires pour lesquelles la CCIN avait saisi le Procureur Général respectivement en 2014 et en 2019.

La première affaire concernait la qualification d'informations nominatives, et les limitations de l'exercice du droit d'accès.

Par jugement en date du 18 mai 2021 le Tribunal Correctionnel a reconnu qu'une donnée de bornage d'un téléphone portable constituait une information nominative au sens de l'alinéa 2

de l'article 1er de la Loi n° 1.165 relative à la protection des informations nominatives aux termes duquel l'information nominative est celle « qui permet d'identifier une personne physique déterminée ou déterminable. Est réputée déterminable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification (...). La Juridiction a ainsi considéré « *qu'une information, telle un numéro de téléphone portable qui est rattaché à une seule personne, dès lors qu'elle permet d'identifier celle-ci, même indirectement, est une information nominative au sens de la loi.* » La collecte et l'enregistrement des données issues des téléphones portables qui ont « accroché » ou activé des bornes étant nécessairement automatiques, l'exploitant de ces équipements revêt la qualité de responsable de traitement, soumis aux obligations en matière de mise en œuvre de traitements automatisés.

Concernant les limitations au droit d'accès aux informations, le Tribunal Correctionnel a relevé que la demande de communication formulée par la personne concernée portait sur « *des renseignements qui relèvent incontestablement des résultats d'une enquête pénale pour avoir été obtenus suite à des réquisitions judiciaires et qui sont donc couverts par le secret prévu à l'article 31 du Code de procédure pénale* » relatif au secret de l'instruction. Aussi il ne pouvait être fait droit à cette demande de communication d'informations.

Dans la seconde affaire le Tribunal Correctionnel a eu tout d'abord à se prononcer sur la validité d'une mission d'investigation conduite par la CCIN en 2018, dont les constatations avaient donné lieu en 2019 à une mise en demeure du responsable de traitement, ainsi qu'à une transmission au Procureur Général.

Les prévenus ont en effet invoqué la nullité des opérations de contrôle sur le fondement des dispositions de l'article 6.1 de la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales garantissant le droit à un procès équitable. L'argument soutenu visait à faire valoir que l'article 18 de la Loi n° 1.165 viole le droit de ne pas participer à sa propre incrimination en gardant le silence en ce qu'il dispose que, dans le cadre de la mission de contrôle de la CCIN, les personnes interrogées sont tenues de fournir les renseignements demandés sauf dans le cas où elles sont astreintes au secret professionnel tel que défini à l'article 308 du Code pénal. En outre, la mention de cette affaire, bien que faite de manière anonymisée, dans le rapport annuel

d'activité de la CCIN pour l'année 2019[4] serait constitutive d'une violation du principe d'égalité des armes et porterait atteinte à la présomption d'innocence et au principe du contradictoire. Cette mention dans le rapport d'activité violerait de plus l'obligation de secret entourant les enquêtes pénales, dans la mesure où le dossier avait été transmis au Parquet.

Aucun de ces arguments n'a été retenu par le Tribunal Correctionnel.

En premier lieu, le Tribunal a, en effet, jugé que les constatations effectuées par les agents investigateurs de la CCIN avaient été de nature purement technique et factuelle. Concernant plus précisément l'article 18 de la Loi n° 1.165, qui impose aux personnes interrogées de fournir, aux agents investigateurs, les renseignements demandés, sauf dans le cas où elles sont tenues au secret professionnel, il a considéré que cette disposition permettait aux membres de la CCIN de procéder à leur mission. Au surplus, le Tribunal a retenu que les constatations des investigateurs avaient été notifiées aux personnes contrôlées, lesquelles disposaient d'un délai suffisant pour faire valoir leurs observations. L'argument tenant à démontrer une rupture de l'égalité des armes n'a dès lors pas prospéré. A l'inverse, il a été considéré que les personnes contrôlées bénéficient de droits identiques à ceux de tous les prévenus et, qu'en l'espèce, les constatations matérielles de la CCIN n'avaient d'ailleurs fait l'objet d'aucune contestation.

Le Tribunal Correctionnel a, en outre, jugé que la publication d'un rapport d'activité annuel ressort d'une obligation légale de la CCIN inscrite à l'article 2, 14° de la Loi n° 1.165. Concernant plus particulièrement la publication litigieuse, il a, au demeurant, constaté qu'elle ne faisait état ni des noms et qualités des prévenus, ni de l'enseigne exploitée et, plus généralement, d'aucune information permettant de les identifier, alors même que la mise en demeure qui leur avait été adressée aurait pu, en vertu de la Loi n° 1.165, être rendue publique.

Les agents qui avaient effectué le contrôle ont été cités à témoin à l'Audience du Tribunal Correctionnel, à la demande du Parquet, afin d'apporter des précisions sur le déroulement des opérations de contrôle dont la validité était contestée par l'Avocat des prévenus.

Les prévenus ont été condamnés au paiement de 1.000 € d'amende chacun pour exploitation illégale d'un traitement automatisé d'informations nominatives, et au versement de 2.400 € de dommages et intérêts au bénéfice des anciens salariés qui s'étaient constitués partie civile, dans la mesure où il a été admis par le Tribunal Correctionnel que les caméras étaient utilisées pour surveiller le travail et le temps de travail des salariés, ce que la CCIN interdit formellement.

[4] Pages 38 et 39 du rapport d'activité 2019

05

L'ACTIVITÉ DE LA CCIN EN LIEN DIRECT AVEC LA CRISE SANITAIRE

LES AVIS SUR LES PROJETS DE DÉCISIONS MINISTÉRIELLES

En 2021 la CCIN a été consultée à 3 reprises, en urgence, par le Ministre d'Etat, sur 5 projets de Décisions Ministérielles, relatives respectivement à une modification de la Décision Ministérielle du 24 février 2020 relative à la situation des personnes présentant des signes d'infection potentielle par le virus 2019-nCoV, à l'instauration d'un passe sanitaire, et à trois modifications successives de la Décision Ministérielle du 20 mai 2020 relative à la mise en œuvre du traitement de suivi de la situation épidémiologique.

Sur le projet de Décision Ministérielle modifiant la Décision Ministérielle du 24 février 2020 relative à la situation des personnes présentant un risque ou des signes d'infection potentielle par le virus 2019-nCoV, prise en application de l'article 65 de l'Ordonnance Souveraine n° 6.387 du 9 mai 2017 relative à la mise en œuvre du règlement sanitaire international (2005) en vue de lutter contre la propagation internationale des maladies

A l'occasion des modifications successives de cette Décision Ministérielle, la Commission avait eu l'occasion d'alerter le Gouvernement en constatant, sans qu'elle en ait été préalablement consultée pour avis, que les établissements hôteliers étaient tenus de procéder à une collecte de données de santé auprès des personnes souhaitant séjourner dans leur établissement. Cette collecte se faisait par le biais d'un document annexé à la Décision Ministérielle concernée, dans lequel les clients devaient renseigner des informations médicales concernant notamment les symptômes listés (présence de toux, de fièvre, de maux de gorge, ...), et indiquer s'ils avaient été récemment malades, ou s'ils l'étaient au moment de leur arrivée. De même la « *production* » du résultat d'un test négatif virologique était demandée, sans qu'il soit précisé s'il convenait de « *présenter* » ce document ou de le « *donner* », les conséquences et l'appréciation de la proportionnalité de la mesure étant différentes en fonction de la définition applicable.

La Commission ayant considéré que ces collectes, effectuées par du personnel non médical, et sans qu'il soit précisé si ces informations faisaient, ou non, l'objet d'une transmission aux Autorités monégasques, étaient disproportionnées, des échanges ont eu lieu avec le Ministre d'Etat, lequel a tenu compte des remarques de la CCIN. Ainsi ce questionnaire s'est mué en une déclaration sur l'honneur, et le résultat d'un test négatif devait être simplement « *présenté* ». La même clarification textuelle a été effectuée en précisant que lors d'un contrôle de police, la personne devait « présenter » le justificatif requis.

C'est dans ce contexte que la Commission a été saisie pour avis, en urgence, le 21 juin 2021, d'un projet de nouvelle modification de la Décision Ministérielle du 24 février 2020, susvisée. Après avoir constaté que les personnes séjournant dans un établissement hôtelier n'auraient désormais plus à remplir d'attestation sur l'honneur, elle a toutefois considéré que les conditions d'accès à

ces établissements n'étaient pas très claires au regard du projet de Décision Ministérielle relative à l'instauration d'un passe sanitaire, lequel projet habilite les exploitants d'hôtel à vérifier le passe sanitaire, tout en prévoyant que le séjour dans un établissement hôtelier dispense de la présentation de ce justificatif pour l'accès à un restaurant, salon de thé,.... Aussi la Commission avait considéré que, dans un souci de prévisibilité, il importait que les conditions d'accès aux hôtels soient plus précises et claires.

Sur le projet de Décision Ministérielle relative au passe sanitaire, prise en application de l'article 65 de l'Ordonnance Souveraine n° 6.387 du 9 mai 2017 relative à la mise en œuvre du règlement sanitaire international (2005) en vue de lutter contre la propagation internationale des maladies

Si la Commission a précisé qu'elle n'était pas en mesure de se prononcer sur la pertinence scientifique du dispositif envisagé, elle a souligné qu'il était nécessaire de mettre en place des garanties suffisantes afin d'assurer que les atteintes aux droits et libertés des personnes concernées, que ce soit le droit à la vie privée, la liberté d'aller et venir ou encore la liberté de consentir à un acte médical, soient nécessaires et proportionnées à l'objectif du dispositif mis en place, à savoir la lutte contre la propagation de la COVID-19.

C'est ainsi qu'après avoir constaté que l'article 1er prévoit que les dispositions de la Décision Ministérielle en projet s'appliquaient jusqu'au 30 septembre 2021 inclus, elle a rappelé que, conformément à l'article 10.1 de la Loi n° 1.165 du 23 décembre 1993, un tel dispositif ne saurait être maintenu au-delà de sa durée nécessaire, c'est-à-dire au-delà de la crise sanitaire actuelle, afin de réduire les risques de contamination.

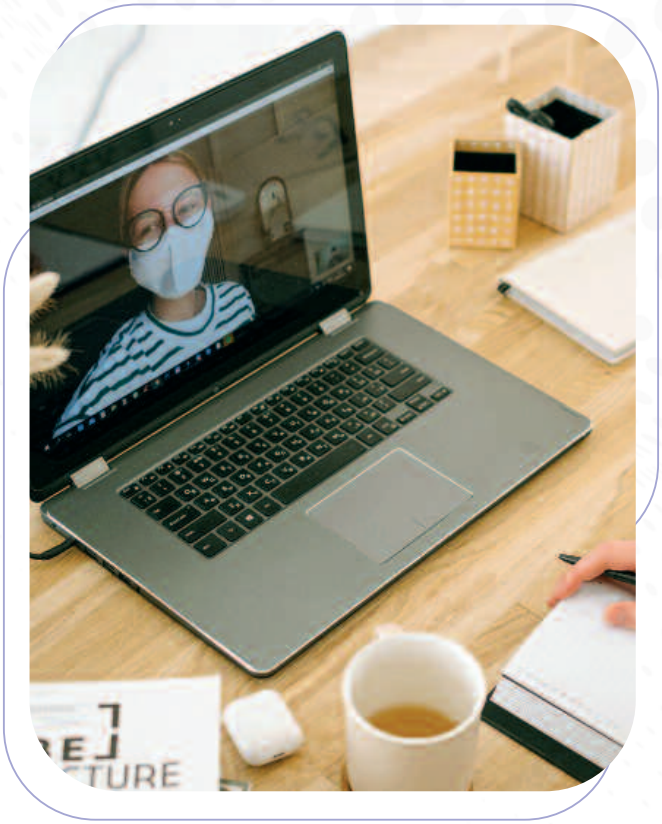
Elle a en effet estimé que le recours à un tel dispositif ne peut s'effectuer que de manière temporaire et exceptionnelle et a, en conséquence, demandé que si l'utilisation de ce dispositif devait être prolongée dans le temps, cette décision soit réévaluée de manière régulière, sur la base des dernières données scientifiques pertinentes disponibles, et documentée.

En ce qui concerne la portée du passe sanitaire, la Commission a constaté que si l'article 7 prévoit, comme dans le Pays voisin, que les établissements, lieux et évènements accueillant un nombre de visiteurs ou de spectateurs au moins égal à

mille personnes sont concernés par le passe sanitaire, ledit article dispose également que l'accès aux établissements ayant des activités sur place de restauration, de bar, de snack, de débit de boissons, de service de petit-déjeuner, de glacier ou de salon de thé ou de café, y compris pour un évènement privé, est également concerné, pour toute personne n'entrant pas dans une des 6 catégories dérogatoires prévues à ce même article (être de nationalité monégasque, résider à Monaco, y être scolarisé ou y travailler, ...).

Aussi, compte tenu des impacts de ce dispositif sur les droits et libertés fondamentaux des personnes, la Commission a estimé que devraient en être exclus les lieux relevant de la vie quotidienne des personnes, tels les restaurants qui sont des lieux que les clients fréquentent de manière habituelle pour passer un bon moment, discuter ou se détendre, afin de minimiser les impacts sur la liberté de réunion des personnes. Elle a en effet relevé que les mesures de restriction d'accès aux établissements concernés ont été mises en place en Principauté plusieurs mois avant l'instauration du passe sanitaire, sans qu'il soit nécessaire de justifier d'un quelconque statut « *Covid 19* ». Aussi elle a estimé que créer une distorsion d'accès à des lieux usuels de vie quotidienne, sur la base de la présentation de documents en lien avec la santé pour une certaine partie de la clientèle seulement - la présentation du passe sanitaire n'étant alors pas requise pour les personnes de nationalité monégasque, pour les résidents de la Principauté ..., notamment - était de nature à créer une atteinte au respect des droits et libertés des personnes.

S'agissant plus globalement des restrictions d'accès auxdits établissements, mises en place depuis plusieurs mois et sur lesquelles la Commission n'avait jamais été consultée, elle a tenu à souligner que même si elle en percevait le fondement en matière de gestion de la crise sanitaire, lesdites restrictions conduisaient les personnels des établissements concernés à effectuer des



vérifications d'identité et de situations (affiliés SPME, CCSS, permis de travail,...) des personnes souhaitant y accéder, lesquelles apparaissent intrusives, et effectuées par des personnes non tenues par une obligation de confidentialité spécifique.

Elle a estimé de plus que la présentation systématique d'une pièce d'identité pour un simple accès à un lieu usuel de la vie courante lui apparaissait disproportionnée. Aussi la Commission a considéré que si ces vérifications devaient perdurer au-delà du 30 septembre 2021, cette décision de maintien devrait également faire préalablement l'objet d'une évaluation approfondie et documentée, sur la base de données scientifiques pertinentes et accessibles.

Sur le consentement des personnes concernées, la Commission s'est félicitée que les utilisateurs aient le choix entre un format numérique et un format papier et puissent à tout moment revenir sur leur choix. A cet effet, elle a souligné l'importance de ne pas discriminer entre les différents supports de justificatifs, afin de ne pas exclure du dispositif une partie de la population qui pourrait,

par exemple, ne pas avoir accès aux outils numériques prévus. Elle a estimé ainsi qu'il pourrait être précisé à l'article 5 que tous ces formats sont d'égale valeur, afin d'éviter qu'un des établissements, lieux ou évènements prévus à l'article 8 ne décide de choisir un support plutôt qu'un autre.

Elle a en outre considéré que les justificatifs en format papier devraient présenter les mêmes garanties que ceux en format numérique, notamment la possibilité pour les détenteurs d'un justificatif papier de ne présenter que le QR code contenant les données numériques, et non les autres informations figurant sur le certificat (statut vaccinal, certificat de rétablissement).

Enfin, concernant l'information préalable des personnes concernées, la Commission a émis le souhait que celle-ci soit effectuée non seulement conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, mais également le plus en amont possible du contrôle, comme par exemple sur les sites de réservation. Elle a également estimé que cette information devrait être standardisée afin d'assurer une information complète et uniforme.

Sur l'extension du passe sanitaire à certains salariés

Concernant la Décision Ministérielle relative au passe sanitaire, la Commission a également été saisie pour avis par le Ministre d'Etat d'un projet de modification visant, notamment, à étendre l'obligation de présentation du passe sanitaire à certaines catégories de salariés, alors que jusque-là cette obligation n'était imposée qu'aux clients ou aux visiteurs.

Cette saisine du Ministre ayant été réceptionnée le 2 décembre 2021, et la Décision Ministérielle ayant été publiée au Journal de Monaco du lendemain, la Commission n'a pas été en mesure d'émettre un avis lors de l'élaboration de cette mesure réglementaire, et donc préalablement à sa publication. Elle a toutefois fait part de ses observations au Ministre d'Etat par un courrier qui lui a été adressé quelques jours après la publication de cette mesure. Elle a ainsi tenu à marquer ses plus vives réserves sur le choix qui a été fait d'étendre cette obligation à des salariés, par le biais d'une Décision Ministérielle prise sur le fondement de l'Ordonnance Souveraine n° 6.387 relative à la mise en œuvre du Règlement Sanitaire International (2005) en vue de lutter contre la propagation internationale des maladies. En effet d'autres Pays liés par ce même Règlement ont considéré qu'il incombait à un texte législatif d'encadrer les restrictions d'accès au lieu de travail pour les salariés. Constatant qu'en application de cette Décision Ministérielle tout salarié

concerné qui n'est pas en mesure de présenter l'un des justificatif requis « *ne peut plus, par l'effet de la présente décision, exercer ses fonctions* », elle a tenu à rappeler, notamment, que l'article 25 de la Constitution garantit la liberté du travail, dont l'exercice est réglementé par la Loi, et a déploré qu'aucun élément précis étayant le caractère proportionné d'une telle atteinte à la liberté du travail, qui plus est par voie réglementaire, ne soit avancé.

Les échanges relatifs à l'extension du passe sanitaire à d'autres salariés se sont poursuivis lorsque le Gouvernement a souhaité modifier à nouveau la Décision Ministérielle du 1er juillet 2021 relative au passe sanitaire, afin cette fois de soumettre à cette obligation « *toute personne dont le travail est indispensable pour la continuité d'activité de certaines entreprises ou de certains services publics assurant des services essentiels à la population* » et dont la liste a fait l'objet d'une publication en annexe de la Décision Ministérielle modificative.

Dans son avis qu'elle a rendu une nouvelle fois dans un délai très contraint, la Commission a souhaité revenir sur le choix du véhicule juridique employé pour étendre une mesure dont l'objectif affiché du Gouvernement est une très forte incitation à la vaccination. En effet les arguments développés auprès d'elle afin de justifier le recours à un texte réglementaire n'ont pas emporté l'adhésion de la Commission.

Elle s'est inquiétée de la situation imprécise de l'ensemble des métiers concernés par cette obligation, dont l'étendue résulte de différentes Décisions Ministérielles intervenues au fil des mois, et dont la portée diffère selon les lieux (chantiers, centre de congrès, exception dans certains cas uniquement pour les livraisons sur des lieux dont l'accès est soumis à la présentation du passe sanitaire, ...). De même la formulation envisagée semblait trop large dans la mesure où l'obligation de présenter un passe sanitaire s'imposait à « *toute personne dont le travail est indispensable pour la continuité d'activité de certaines entreprises ou de certains services publics assurant des services essentiels à la population* ». Aussi la Commission a suggéré de modifier le projet de Décision Ministérielle en indiquant que cette obligation concerne les seules personnes dont l'activité concourt aux services essentiels à la population. Là encore l'avis de la Commission n'a été que très partiellement pris en compte, la formulation définitive imposant cette obligation à « *toute personne dont l'exercice professionnel est indispensable pour la continuité d'activité d'une entreprise ou d'un service public assurant des services essentiels à la population.* »

Enfin, dans un souci de cohérence des obligations imposées aux salariés par le biais de différentes Décisions Ministérielles, la Commission a souligné qu'il conviendrait de préciser que l'obligation de présentation du passe sanitaire ne s'appliquait pas aux personnes effectuant l'intégralité de leur prestation à distance en application de la Décision Ministérielle du 30 décembre 2021 relative à l'adoption de conditions de travail à distance obligatoire pour les salariés, fonctionnaires, agents de l'Etat ou de la Commune, et ce pour tout ou partie de la durée hebdomadaire de travail. Cette remarque n'a pas trouvé écho auprès du Gouvernement.

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

La Commission a, au cours de l'année 2021, rendu trois avis concernant des projets de Décisions Ministérielles modifiant la Décision Ministérielle du 20 mai 2020 relative à la mise en œuvre d'un traitement d'informations nominatives destiné à permettre le suivi de la situation épidémiologique, prise en application de l'article 65 de l'Ordonnance Souveraine n° 6.387 du 9 mai 2017 relative à la mise en œuvre du règlement sanitaire international (2005) en vue de lutter contre la propagation internationale des maladies.

La première saisine a concerné l'intégration des données relatives à la vaccination contre la Covid-19. Dans son avis rendu par délibération n° 2021-001 en date du 13 janvier, la Commission s'est notamment interrogée sur le contenu de « *la fiche de traçabilité* », regrettant que celui-ci ne soit pas détaillé afin de faire une distinction claire entre les éléments nécessaires au suivi administratif de la campagne de vaccination et ceux relatifs à la pharmacovigilance.

Après avoir relevé que l'article 7 de la Décision Ministérielle du 30 décembre 2020 relative à la vaccination contre la COVID-19 prévoit que ladite fiche contient l'identification de la personne vaccinée, la dénomination commerciale du vaccin administré, la date de son administration et son numéro de lot de fabrication, l'identification du vaccinateur, le site d'injection du vaccin et la date prévisionnelle du rappel lors de la primo injection, la Commission aurait en effet souhaité que le terme « *identification de la personne vaccinée* » soit défini afin de préciser quelles données personnelles pouvaient être concernées, comme par exemple les nom, prénoms, sexe, date et lieu de naissance de ladite personne, ses coordonnées ou encore, le cas échéant, les noms et coordonnées de son représentant légal.

Par ailleurs, après avoir noté que le plan de vaccination contre la COVID-19 établi par l'Etat prévoit une priorisation des catégories de population à vacciner, la Commission s'est demandée si des informations de santé telles que les critères médicaux d'éligibilité à la vaccination et les traitements suivis ne seront pas également collectés. De même, elle a considéré probable que les effets indésirables associés à la vaccination seront également renseignés sur lesdites fiches.

Concernant les accès au traitement, la Commission a rappelé que les extractions procédées par les médecins-inspecteurs devaient être sécurisées.

Elle a par ailleurs réitéré ses réserves concernant l'accès des personnels techniques, voire administratifs, à la base, et rappelé qu'aux termes de sa délibération 2020-084 portant avis sur le projet de Décision Ministérielle relative à la mise en œuvre d'un traitement d'informations nominatives destiné à permettre le suivi de la situation

épidémiologique, prise en application de l'article 65 de l'Ordonnance Souveraine n° 6.387 du 9 mai 2017 relative à la mise en œuvre du Règlement Sanitaire International (2005) en vue de lutter contre la propagation internationale des maladies, elle a considéré « qu'en l'absence de circonstances particulières pouvant justifier une telle atteinte au secret médical, la base de données devrait être chiffrée sur les serveurs de la Direction des Réseaux et des Systèmes d'Information (DRSI), et que les personnels de cette Direction ne devraient pas pouvoir accéder en clair également aux résultats des tests sanguins lors de leur réception en provenance des laboratoires « *partenaires* » ». Cela est d'autant plus vrai en ce qui concerne la décision par les personnes concernées de se faire vacciner, ou non.

Enfin, après avoir relevé que le nouvel article 4 en projet précisait en son alinéa 1er que les accès s'effectuent « *dans la stricte mesure où leur intervention est nécessaire et dans la limite des seules informations nécessaires à leur intervention* », insérant ainsi directement dans le dispositif l'accès selon le besoin d'en connaitre, la Commission a également constaté que les accès aux fins de suivi de la traçabilité des vaccinations et de suivi du taux de couverture vaccinale avaient été prévus en cohérence avec l'introduction des vaccins dans le suivi épidémiologique.

Concernant les durées de conservation, elle s'est interrogée sur l'actualisation de la base de données et la pertinence dans le temps des informations objets du traitement. En effet, la période de crise se prolongeant, les personnes initialement concernées ne l'étaient peut-être plus (perte d'emploi, décès, etc.), tandis que de nouvelles personnes auraient pu intégrer la base (nouveaux élèves scolarisés, etc.). Or, n'avait été évoquée à ce stade qu'une seule communication initiale des données issues de différents traitements tenus parfois par des responsables de traitements tiers (CCSS, Mairie) permettant la constitution de la liste prévue au point 1) de l'article premier. Ces données « *source* », une fois la liste constituée, ont été supprimées. Aussi, la Commission a souligné la nécessité que cette liste soit tenue à jour, selon des modalités sécurisées et périodiques, emportant la suppression des informations obsolètes et des fichiers « *source* ». D'autre part, elle a estimé que les personnes initialement concernées mais sorties de la liste et qui n'ont pas fait l'objet de tests, devraient alors être supprimées.

Enfin, à la lecture du projet de nouvel article 6, elle a relevé qu'au 1er janvier 2022 les informations relatives aux :

- personnes n'ayant pas été testées ou vaccinées seront anonymisées. Sauf besoin statistique particulier, elle considère qu'elles pourraient être supprimées.
- personnes testées mais non vaccinées seront anonymisées.
- personnes vaccinées seront conservées, qu'il s'agisse de la fiche de traçabilité du vaccin inoculé ou des tests effectués.

Concernant cette dernière catégorie de personnes, la Commission s'est interrogée sur la pertinence de conserver l'historique des tests qu'elles ont réalisés. Si elle peut comprendre l'intérêt de garder pendant une certaine durée postérieure à la vaccination d'une personne le fait de savoir si elle a ou non effectué de nouveaux tests et leurs résultats, afin de vérifier si le ou les vaccins inoculés sont efficaces contre la Covid-19, elle a estimé que les informations relatives aux tests devraient être anonymisées avant la durée de 20 ans. Aussi, la Commission a estimé qu'au 1er janvier 2024, après une période de deux ans ayant permis de déterminer quels sont les vaccins les plus efficaces, les fiches de traçabilité des vaccins soient décorrélées des informations relatives aux tests. Toutefois, si des raisons spécifiques devaient justifier une durée de conservation plus longue, la Commission serait alors bien évidemment à l'écoute du Gouvernement.

Dans son deuxième avis rendu en date du 23 juin 2021 par sa délibération n° 2021-144, la Commission a tout d'abord relevé que l'article 1er prévoit que vont être désormais également intégrées au traitement objet de la Décision Ministérielle, les données d'identification des personnes ayant été en contact avec des personnes atteintes par le virus afin d'identifier, au moyen d'une enquête sanitaire si nécessaire, les personnes présentant un risque d'infection.

Si elle a considéré que ces données sont en adéquation avec la finalité du traitement, limitée au suivi de la situation épidémiologique, la Commission a estimé qu'une durée de conservation de quelques jours de ces données devrait être prévue afin de ne pas conserver ces informations au-delà de la durée nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées.

Cette remarque a partiellement été prise en compte dans la version définitive du texte en date du 1er juillet 2021 puisque l'article 6 prévoit que « *Les données d'identification des personnes ayant été en contact avec des personnes infectées par le virus SARS-CoV-2 sont conservées pendant trois mois à compter de la date du résultat positif d'un test du cas index* ».

La Commission a tenu à souligner par ailleurs qu'une politique stricte d'habilitations devait être mise en place afin que seules les personnes ayant à connaître de ces données puissent y avoir accès, les cas contacts relevant en effet fréquemment de la sphère privée des personnes concernées.

Elle a également relevé que l'article 6 en projet prévoyait que toutes les « *informations nominatives contenues dans le traitement mentionné à l'article premier et afférentes à la vaccination contre la COVID-19 et au résultat de tout test mentionné audit article sont conservées, pour chaque personne vaccinée, pendant une durée de vingt ans à compter de sa dernière vaccination* ».

A cet égard, la Commission a pris acte des précisions du responsable de traitement selon lesquelles « *Il est nécessaire de conserver l'historique des tests réalisés, dans le cadre du suivi de la crise sanitaire, si la personne est réinfectée et si une personne vaccinée contracte de nouveau le virus ou un de ses variants* ».

Enfin, sur la sécurité et la confidentialité de la base de données, elle a rappelé que, compte tenu de leur sensibilité, les données contenues dans cette base devraient être chiffrées, et ce d'autant plus que depuis la création de cette base, initialement dévolue aux campagnes de dépistage TROD, celle-ci a été enrichie de nombreuses données de santé (antécédents médicaux, statut vaccinal, ...) et prochainement des cas contacts des personnes concernées, relevant pour l'essentiel de leur sphère privée de connaissance.

En conséquence, en l'absence de chiffrement des données contenues dans la base, et au regard des nombreux accès par des Directions supports, la Commission a estimé que les Directions opérationnelles, en charge du suivi des différentes fonctionnalités du présent traitement, devraient être informées des accès effectués par les Directions supports, et des motifs de ceux-ci (maintenance, support utilisateur, ...). Une telle information devrait parallèlement être délivrée aux hiérarchies des personnes des Directions supports ayant effectué ces accès.

A cet effet, la Commission a là encore rappelé que les accès des personnes habilitées doivent être restreints et strictement dévolus en considération des missions et des fonctions des personnes auxquelles ils sont attribués, conformément aux articles 8 et 17 de la Loi n° 1.165 du 23 décembre 1993.

La troisième saisine portant sur un nouveau projet de modification de la Décision Ministérielle du 20 mai 2020 relative à la mise en œuvre d'un traitement d'informations nominatives destiné à permettre le suivi de la situation épidémiologique a été effectuée en toute fin d'année 2021.

Cette nouvelle modification concernait le report d'une année de la date d'anonymisation des informations relatives aux personnes non vaccinées, laquelle devait initialement intervenir au 31 décembre 2021.

Par délibération n° 2021-278 du 15 décembre 2021 la Commission a rappelé que les données ayant servi à l'incrémentation initiale de cette base, au printemps 2020, n'avaient semble-t-il jamais été mises à jour. Dans sa délibération n° 2021-001 du 13 janvier 2021, précitée, elle s'inquiétait déjà du défaut d'actualisation de la base de données initiale, et donc de la pertinence dans le temps de l'intégralité des informations objets du traitement. En effet les personnes initialement concernées ne le sont peut-être plus (perte d'emploi, ...) tandis que de nouvelles personnes sont désormais concernées (nouveaux élèves scolarisés, nouveaux résidents ou salariés, ...).

Aussi, elle a considéré que le report d'une année supplémentaire de l'anonymisation des données devrait donner lieu à une actualisation de cette base, cette mise à jour étant de plus de nature à disposer d'une vision plus exacte et actualisée du suivi épidémiologique de la population.

Sur la pertinence de ce report, elle a souligné que le projet de Décision Ministérielle objet de sa saisine précisait « *Considérant que l'état de la menace sanitaire liée au risque épidémique en cours nécessite de retarder au 31 décembre 2022 la date à laquelle devaient être anonymisées certaines données contenues dans le traitement automatisé d'informations nominatives autorisé par la Décision Ministérielle du 20 mai 2020* », et en a pris acte.

LE PROJET DE LOI RELATIVE À L'OBLIGATION VACCINALE

La Commission n'a pas été saisie, pour avis, par le Ministre d'Etat de ce projet de Loi alors même que l'article 2 alinéa 2 de la Loi n° 1.165 relative à la protection des informations nominatives dispose qu'elle « *est consultée par le Ministre d'Etat lors de l'élaboration de mesures législatives ou réglementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement des informations nominatives (...)* ».

Après avoir pris connaissance de ce projet de texte, comme tout un chacun, sur le site Internet du Conseil National, la Commission a souhaité appeler l'attention du Ministre d'Etat, par courrier, sur certains points ayant des incidences en matière de traitement des données personnelles et de préservation des droits des personnes concernées par les dispositions envisagées.

Elle a ainsi relevé des terminologies mentionnées dans ce projet que les personnes soumises à l'obligation vaccinale doivent justifier de leur statut, produire les justificatifs requis, présenter les documents relatifs à la dispense d'obligation vaccinale tout en justifiant de l'un des deux motifs de dispense, sans qu'il soit précisé de manière explicite si les obligations envisagées induisent une remise de document à des fins de conservation par les responsables des entités concernées, ou une simple présentation des justificatifs visés. Aussi elle a considéré que des précisions devaient être apportées sur ce point, ce qui a été fait par le biais des amendements apportés lors des débats législatifs. En effet le texte définitif mentionne explicitement la transmission des documents requis, soit à l'employeur, soit à l'Office de la Médecine du Travail.

S'agissant des personnes soumises à l'obligation vaccinale exerçant à titre libéral, dont les autorisations d'exercice et les abrogations d'autorisations donnent lieu à des publications au Journal Officiel, elle s'est inquiétée que les motifs de suspension administrative d'exercice du fait de leur décision de ne pas se faire vacciner donnent lieu à publication, au mépris du droit au respect de la vie privée.

N'ayant pas reçu de réponse à son courrier, la Commission a toutefois constaté que si des mesures de suspension avaient été prises, aucune publication des motifs de ces suspensions n'a été faite, ce qui l'a rassurée.

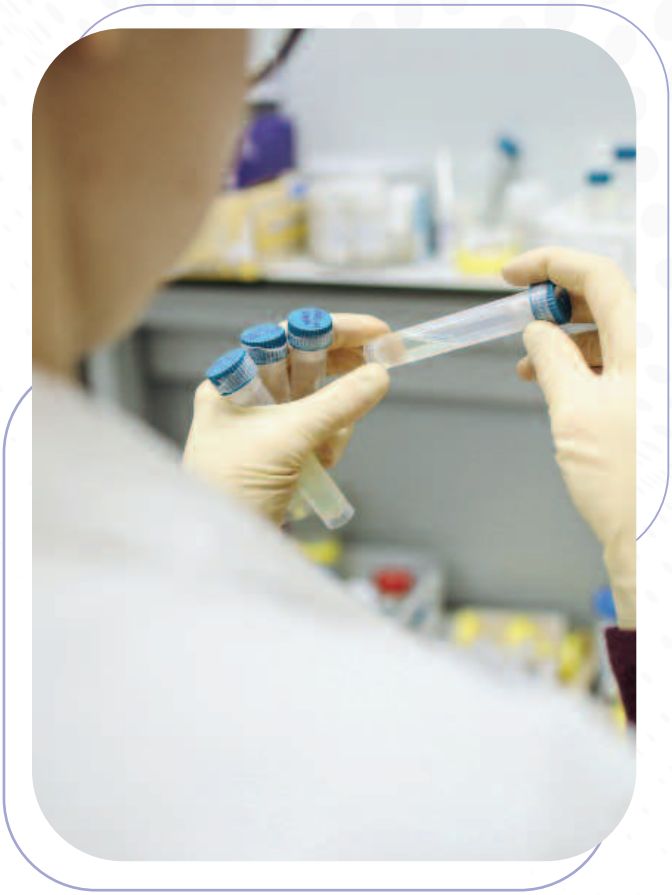
LES RECHERCHES BIOMÉDICALES EN MATIÈRE DE COVID 19

Le 20 janvier 2021, la Commission a émis 2 avis favorables concernant des recherches biomédicales, en lien avec le Covid-19.

- La première de ces recherches, présentée par le Centre Hospitalier Universitaire d'Angers représenté à Monaco par le Centre Hospitalier Princesse Grace, est dénommée « *Revise-dHOME-CoV* ».

Cette étude concerne plusieurs centres hospitaliers en France, en Belgique et à Monaco. En Principauté, cette étude se déroulera au CHPG, sous la responsabilité d'un médecin investigateur exerçant au sein de l'unité COVID Urgences. Le responsable de traitement souhaite inclure 1300 patients au total dont 20 à Monaco.

Elle a pour objectif principal de démontrer la fiabilité et la sécurité de la prise en charge ambulatoire chez les patients hautement suspects ou confirmés atteints de la COVID-19 se présentant aux urgences et ayant un score HOME-CoV révisé inférieur à 2 (règle négative).



Le traitement automatisé concerne donc, au principal, les patients suivis dans l'unité COVID Urgences ainsi que les médecins investigateurs, les attachés de recherche clinique (ARC) et les personnels intervenant au cours de l'étude sur autorisation du médecin investigateur.

Ses fonctionnalités sont :

- organiser l'inclusion des patients ;
- collecter et analyser les données des sujets conformément aux objectifs scientifiques et au protocole de l'étude ;
- conserver les données traitées dans le respect des réglementations applicables ;
- assurer la sécurité de l'étude en veillant, notamment, à l'identification des acteurs de la recherche, la qualité et la traçabilité des données, ainsi que celles des actions automatisées réalisées ;
- permettre, le cas échéant, le suivi des effets indésirables.

D'une durée de seulement 3 mois et 2 semaines, elle n'a fait l'objet d'aucune remarque particulière de la Commission.

- La deuxième étude, présentée cette fois par le Centre Hospitalier Régional d'Orléans, a pour objectif principal de montrer que le décubitus ventral (DV) chez les patients en ventilation spontanée « *permet de diminuer le risque d'acquérir l'évènement suivant qui peut être vu comme un critère composite :*
- *Intubation endotrachéale*
- *Ou ventilation non-invasive à deux niveaux de pression*
- *Et/ou Décès* ».

Dénommée « *PROVID19* », elle doit concerner 400 patients au total dont 20 suivis au sein de l'unité COVID du CHPG

Le traitement automatisé concerne donc, au principal, les patients suivis dans l'unité COVID ainsi que les médecins investigateurs, les attachés de recherche clinique (ARC) et les personnels intervenant au cours de l'étude sur autorisation du médecin investigateur.

Ses fonctionnalités sont les suivantes :

- organiser l'inclusion des patients ;
- collecter et analyser les données des sujets conformément aux objectifs scientifiques et au protocole de l'étude ;
- conserver les données traitées dans le respect des réglementations applicables ;
- assurer la sécurité de l'étude en veillant, notamment, à l'identification des acteurs de la recherche, la qualité et la traçabilité des données, ainsi que celles des actions automatisées réalisées ;
- permettre, le cas échéant, le suivi des effets indésirables.

Après avoir relevé que la notice d'information prévoit qu'en l'absence d'opposition de la part du patient, les données collectées dans le cadre de cette recherche seront conservées « *afin d'être réutilisées pour d'autres études rétrospectives jusqu'à 15 ans après la fin de cette étude* », la Commission a demandé que cette utilisation des données collectées dans le cadre de la présente recherche pour des études futures fasse l'objet d'un consentement séparé par le biais d'une case à cocher au sein du formulaire de consentement, afin que le patient puisse effectivement y consentir ou s'y opposer.

LA MISE EN ŒUVRE DE TRAITEMENTS RÉSULTANT DE LA CRISE SANITAIRE

Les modifications apportées au traitement de suivi de l'évolution du SARS-COV-2

Au mois de juin 2020 la Commission avait été saisie d'une demande d'avis relative à la mise en œuvre, par le Département des Affaires Sociales et de la Santé, d'un traitement dont la finalité initiale était de suivre la campagne de dépistage du Covid-19 au moyen de Tests Rapides d'Orientation du Diagnostic (TROD). La mise en œuvre de ce traitement s'inscrivait dans le cadre de la Décision Ministérielle du 20 mai 2020, dont de nombreuses modifications ultérieures ont élargi le périmètre initial des fonctionnalités du traitement y afférent.

C'est dans ce cadre que la Commission a été saisie pour avis, au mois de juin 2021, d'une modification du traitement communément appelé « *Base de données Covid-19* ».

Cette base de données s'est enrichie au fil des mois et contient, outre les éléments portés initialement à la connaissance de la CCIN, le suivi de la vaccination, la plateforme de prise de rendez-vous, le suivi à domicile des patients, l'application mobile de consultation des résultats des tests, les antécédents médicaux communiqués volontairement par les personnes testées qui participent à l'étude appelée « *cordage* » et dont la Commission a estimé qu'elle devait faire l'objet d'un traitement distinct au regard des données médicales y figurant. Les dernières évolutions de cette base de données, au mois de juin 2021, ont concerné les développements nécessaires à la mise en œuvre du passe sanitaire.

La Commission a souligné que les fonctionnalités de cette base de données, de plus en plus nombreuses, vont bien au-delà de la finalité du traitement de « Suivi de l'évolution du SARS-COV-2 de la Principauté », ce qui ne contribue pas à sa lisibilité pour les personnes concernées, et permet difficilement à la Commission de s'assurer de la légitimité des accès par les différents Services en charge de l'exploitation de cette base. Aussi elle a estimé souhaitable de scinder cette base de données en différents traitements correspondant explicitement à leurs objectifs spécifiques.

S'agissant plus particulièrement de l'intégration du passe sanitaire, elle a acté que les personnes concernées auront la possibilité de donner leur accord afin que le certificat monégasque soit converti en certificat français, par le biais d'une communication à la France afin de bénéficier d'une reconnaissance à l'étranger de leur statut. Dès la conversion opérée en France, les données nominatives seront aussitôt supprimées par le responsable de traitement français. Les Services de la CCIN avaient été contactés par le Référent RGPD de la Direction Générale de la Santé (DGS) française afin d'obtenir des précisions sur les flux de données qui seraient opérés entre la Principauté et le Pays voisin, Monaco ne disposant en effet pas d'une reconnaissance de protection adéquate, par l'Union européenne, en matière de données

personnelles. Ceci nécessite donc la mise en place de garanties spécifiques en cas de transfert d'informations en direction de la Principauté. Les précisions qui ont été apportées aux Services de la DGS ont permis de répondre à leurs questionnements en matière de protection des données personnelles.

Enfin, la base de données n'étant toujours pas chiffrée, la Commission a demandé la mise en place d'une procédure d'information des Directions métiers en cas d'accès par les Directions supports, et ce afin de s'assurer que ces accès sont effectués dans le strict cadre de l'accomplissement de leurs missions.

Les enquêtes épidémiologiques COVID-9 en milieu de travail de l'Office de la Médecine du Travail

Au mois de juillet 2021 la Commission a émis un avis favorable à la mise en œuvre, par l'Office de la Médecine du Travail (OMT) d'un traitement destiné à suivre et à gérer les personnes testées positives à la Covid-19, afin d'organiser des campagnes de dépistage des cas contacts sur le lieu de travail. Ce traitement s'inscrit dans le cadre de la Décision Ministérielle du 5 janvier 2021 relative à l'adaptation des règles relatives à la médecine du travail dans le cadre de l'épidémie Civid-19, qui est venue conforter le rôle et les missions de l'OMT face à cette pandémie. Il résulte également d'une procédure mise en place par la Direction de l'Action Sanitaire (DASA) qui associe l'employeur à la gestion de la crise sanitaire.

Ceci a conduit la Commission à appeler l'attention sur le risque que l'employeur ne mette pas en œuvre la confidentialité requise concernant l'identité du cas « *index* » qui souhaite peut-être que ce statut ne soit pas connu de ses collègues de travail. Aussi elle a demandé que les employeurs soient plus particulièrement sensibilisés sur ce point.

Elle a acté que la transmission des données nominatives par l'OMT à la DASA était sécurisée, et que l'OMT mettait à disposition des employeurs une messagerie sécurisée aux fins de communiquer les tableaux nominatifs des cas contacts.

Concernant les durées de conservation des données, elles sont anonymisées après 2 mois, mis à part les résultats des tests qui, ayant été prescrits par les Médecins de l'OMT, sont conservés dans le dossier médical des salariés concernés.

Le suivi de la vaccination des employés et des personnes intervenant au CHPG

Par délibération n° 2021-206 du 20 octobre 2021, la Commission a émis un avis favorable à la mise en œuvre du traitement ayant pour finalité « *Suivi de la vaccination des employés du CHPG contre la COVID-19* », sous réserve cependant de la prise en compte de ses nombreuses observations.

Elle a ainsi relevé que l'article 1er de la Loi n° 1.509 du 20 septembre 2021 relative à l'obligation vaccinale contre la COVID-19 de certaines catégories de personnes prévoit que tout membre d'un établissement de soins ou de santé est tenu d'être vacciné contre la COVID-19.

La Commission a par ailleurs noté qu'en vertu de cette même Loi, « *toute personne soumise à l'obligation vaccinale qui ne pourra pas justifier de son accomplissement ou prouver qu'elle s'est rétablie à la suite d'une contamination par le virus de la COVID-19, sera suspendue de ses fonctions* ».

Elle a également constaté que le présent traitement a notamment pour objectif d'effectuer un suivi dynamique des situations des personnes concernées par l'obligation vaccinale, et que ce suivi permettra d'appliquer les dispositions légales prévues en cas de non justification d'un schéma vaccinal complet, d'un certificat de rétablissement ou de confirmation de contre-indication.

S'agissant des catégories de personnes concernées par le présent traitement la Commission a souligné qu'en application du chiffre 2 de l'article 1er de la Loi n° 1.509, susvisée, l'obligation vaccinale concerne : « *toute personne qui, sans être membre du personnel de l'un des établissements, services ou organismes mentionnés au chiffre 1), y exerce une activité, y compris à titre de bénévole, d'élève ou d'étudiant, lorsqu'elle est en contact direct avec des personnes qu'il accueille, encadre ou héberge, à l'exclusion de celle qui exerce ponctuellement cette activité sans être en contact direct avec des personnes qu'il accueille, encadre ou héberge* ».

Aussi elle a demandé que le périmètre des personnes concernées par le présent traitement soit conforme aux dispositions légales.

Concernant le statut vaccinal de l'agent, la Commission a rappelé que les personnes soumises à l'obligation vaccinale ont la possibilité de justifier de leur situation soit directement auprès du CHPG, soit auprès, selon les cas, de l'Office de la Médecine du Travail (OMT) ou de la Direction de l'Action Sanitaire (DASA), à charge pour ces deux entités d'informer le CHPG de la satisfaction par les personnes concernées à l'obligation vaccinale telle que définie par les articles premier et 2 de la Loi n° 1.509.

Aussi, elle a tenu à souligner que la mention de cette information par l'OMT ou la DASA doit être portée dans le présent traitement, à l'exclusion dans ce cas d'autres indications justifiant du statut des personnes concernées.

Par ailleurs, sur l'information préalable des personnes concernées, la Commission a pris note que celle-ci était réalisée par le biais de la « *Politique générale de la protection des données à caractère personnel des professionnels du CHPG* » disponible sur l'Intranet du CHPG.

Toutefois après avoir relevé que certaines catégories de personnes soumises à l'obligation vaccinale ne sont pas salariées du CHPG, ou n'ont pas accès à l'Intranet de l'établissement, la Commission a demandé que l'information de toutes les personnes concernées soit valablement effectuée.

S'agissant du rapprochement de ce traitement avec la messagerie professionnelle, la Commission a relevé que celle-ci permet donc la collecte et la transmission des justificatifs médicaux. En conséquence, compte tenu du caractère sensible de ces données, elle a demandé que ces communications soient traitées dans les plus brefs délais puis supprimées de la messagerie.

Elle a demandé que cette suppression soit également effectuée sur le système de sauvegarde de la messagerie.

Enfin, concernant les durées de conservation des données, la Commission a constaté que les informations liées à la vaccination sont conservées, conformément à la Loi n° 1.509 du 20 septembre 2021, 18 mois à compter du 30 octobre 2021, et que

si les délais devaient être raccourcis, les données seraient supprimées. A cet égard, la Commission a rappelé que si les délais devaient en revanche être allongés, une demande de modification du présent traitement devra lui être soumise.

LA DÉFENSE DES DROITS DES PERSONNES CONCERNÉES

Sans que cela ait donné lieu à des plaintes, la CCIN a toutefois été informée de pratiques non conformes en matière de préservation de la vie privée, mises en place par certains employeurs, et qui ont nécessité son intervention rapide afin d'y mettre un terme sur le champ.

Cela a concerné en premier lieu la campagne de vaccination, dans le cadre de laquelle des entités ont adressé à leurs Agents un questionnaire, nominatif, leur demandant s'ils avaient été vaccinés (auquel cas il leur était demandé de joindre la copie de leur attestation de vaccination) ou pas, et s'ils souhaitaient bénéficier de la possibilité de bénéficier d'une vaccination à Monaco, et ce en dehors de toute obligation légale de vaccination, ou de soumission à l'obligation de présentation d'un passe sanitaire pour accéder à leur lieu de travail.

Si la diffusion de ce questionnaire avait pour vocation de permettre aux Agents volontaires de pouvoir bénéficier d'une telle vaccination, qui n'était alors ouverte qu'aux seuls résidents de la Principauté, le modus operandi était totalement intrusif, et le quantum des informations demandées bien trop large.

Aussi la CCIN est intervenue et il a été mis fin à la diffusion de ce questionnaire. Elle a suggéré qu'en lieu et place, une information globale soit diffusée auprès des Agents afin de les informer de cette possibilité de se faire vacciner en Principauté, libre à ceux qui le souhaitaient de pouvoir en bénéficier, ou non.

Le second signalement a concerné l'extension du passe sanitaire à certaines catégories de salariés, objet d'une Décision Ministérielle publiée le 3 décembre 2021, qui étendait l'obligation de présentation du passe sanitaire pour l'accès à certains lieux, y compris pour les salariés y travaillant.

Là aussi la CCIN a été informée de l'obligation faite par certains employeurs de demander la présentation du passe sanitaire à leurs salariés, et ce alors même que la Décision Ministérielle ne le prévoyait pas. Là aussi l'intervention de la CCIN auprès des employeurs concernés a permis de mettre fin à ces pratiques illégales.

Suite à ces signalements émanant de salariés la CCIN a publié un communiqué sur son site Internet afin de préciser les bonnes pratiques à respecter en matière de passe sanitaire, et plus largement de respect des dispositions légales en matière d'obligation vaccinale de certaines catégories de salariés. Ce communiqué a été mis à jour à plusieurs reprises afin de tenir compte des nouvelles Décisions Ministérielles publiées au fil des mois[5].

[5] Ce communiqué est disponible sur le site Internet de la CCIN www.ccin.mc

06

LA MISE EN ŒUVRE DE L'IDENTITÉ NUMÉRIQUE

En 2021, et dans une extrême urgence alors même que le projet d'instauration d'une identité numérique en Principauté avait donné lieu à des réunions préparatoires depuis trois ans, la CCIN a été saisie pour avis, de manière concomitante, des projets de textes réglementaires indispensables à l'assise textuelle de l'instauration de l'identité numérique, et de la mise en œuvre des traitements associés.

LES AVIS DE LA COMMISSION SUR LES PROJETS DE TEXTE RELATIFS À L'IDENTITÉ NUMÉRIQUE

Les trois projets d'Ordonnance Souveraine portant application de différents articles de la Loi n° 1.483 relative à l'identité numérique

La CCIN a été saisie pour avis, par SEM le Ministre d'Etat, de trois projets d'Ordonnances Souveraines portant application de divers articles de la Loi n° 1.483 relative à l'identité numérique.

En préambule de son avis, la CCIN a tenu à rappeler qu'elle s'était prononcée, en 2019, sur un projet de Loi, centré, à l'époque, autour d'une vision régalienne de l'identité numérique, accessible aux seuls nationaux et résidents et qui ne contenait que 10 articles[6] .

Or, la Loi n° 1.483, qui en comporte finalement 20, a substantiellement élargi le périmètre de l'identité numérique pour l'étendre à d'autres catégories de personnes, ce qui a conduit la Commission à formuler un certain nombre de remarques.

Sur le périmètre de la Loi n° 1.483 relative à l'identité numérique

La Commission s'est ainsi questionnée, tant sur le périmètre effectif de la Loi n° 1.483, susceptible de constituer une insécurité juridique, que sur l'absence d'encadrement des fournisseurs de services et du moyen d'authentification « *MConnect* ».

Concernant le périmètre de la Loi, s'il a semblé à la Commission que l'objectif affiché de l'identité numérique était de permettre l'accès aux services en ligne de l'administration, la définition générale et universelle de celle-ci, telle que consacrée à l'article 2 de la Loi n° 1.483, ne lui a cependant pas permis de s'en assurer.

Du reste, la Commission a observé une confusion, au moins partielle, entre le périmètre de l'identité numérique et celui de la Loi pour une Principauté Numérique. Au terme de ce dernier texte, la signature électronique qualifiée, définie comme étant constituée de données d'identification personnelle sous une forme numérique représentant, de manière univoque, une personne physique, constitue en effet, au sens de l'article 2 de la Loi n° 1.483 une identité numérique.

Compte tenu de la définition générique de l'identité numérique consacrée à l'article susvisé, la Commission s'est légitimement questionnée sur la possibilité, pour un opérateur privé, de délivrer une identité numérique (par exemple en proposant une signature électronique qualifiée) autrement qu'en application des dispositions de la Loi n° 1.483.

[6] Voir rapport d'activité 2019 page 59 et suivantes

Vu la nomenclature précise permettant de constituer l'identité numérique et le nombre limité d'informations pouvant être collectées par les fournisseurs d'identité, la Commission n'a, de plus, pas compris l'insertion, à l'article 2 de la Loi n° 1.483, des données biométriques.

Elle a, en outre, regretté l'absence d'encadrement des fournisseurs de services et de l'authentification MConnect (MConnect). Elle a d'ailleurs souligné que la notion de « *Fournisseurs de Services* » *lui semble venir se substituer aux « plateformes de service et d'administration électronique* » consacrées par la Loi n° 1.483. A l'analyse des traitements qui lui ont été concomitamment soumis en matière d'identité numérique, la Commission a constaté la possibilité technique d'implémenter MConnect sur les services en ligne proposés par les fournisseurs de services pour que l'identité numérique des nationaux et résidents soit reconnue. La Commission a fortement regretté qu'une définition des fournisseurs de services ne soit proposée qu'au détour d'un article du projet d'Ordonnance Souveraine portant application des articles 6,8 et 13 de la Loi n° 1.483, lesquels sont entendus comme « un service en ligne proposé aux usagers ». La Commission a noté à cet égard que cette définition, liée aux services exécutifs de l'Etat, tout comme la référence faite aux usagers, pourrait laisser penser que le fournisseur de services correspond à une e-administration. Elle s'est, dès lors, interrogée sur la possible étendue, à court ou moyen terme, de l'authentification MConnect aux autres entités publiques ou privées qui désireraient bénéficier de ce moyen d'identification numérique.

L'insertion des services de confiance dans le dispositif de la Loi n° 1.483

La Commission s'était déjà inquiétée en 2019 de l'insertion des services de confiance dans le dispositif de la Loi sur l'identité numérique. En l'occurrence, elle a constaté que la définition de service de confiance inscrite dans la Loi n° 1.483 diffère de celle de la Loi pour une Principauté numérique. Si la première précise que les services de confiance consistent notamment en une « identité », la seconde consacre les termes d'« *identification numérique ou une authentification* ». En outre, le fournisseur d'identité est qualifié, par la Loi n° 1.483, de prestataire de service de confiance sans qu'il soit possible de connaître la nature dudit service de confiance.

La Commission s'est pareillement étonnée de l'absence de registre permettant de recenser les fournisseurs d'identité autorisés bien que ces derniers seront inscrits sur la liste des services de confiance établie, en application de la Loi pour une Principauté numérique.

Sur la nécessaire clarification des interactions entre les différents acteurs de l'identité numérique monégasque

La Commission a exprimé ses inquiétudes portant sur la logique soutenant les évolutions futures de l'identité numérique monégasque. En application de la Loi n° 1.483, cette dernière devrait, à terme, pouvoir être élargie aux acteurs du service public et du secteur privé.

De ce fait, la Commission a estimé nécessaire que des clarifications soient apportées, tant sur les personnes éligibles à une identité numérique

garantie par l'Etat pour accéder notamment à son « *administration électronique* », que sur le rôle du Registre National Monégasque de l'Identité Numérique créé par la Loi n° 1.483 (RNMIN) et celui des fournisseurs d'identité monégasque.

Concernant plus précisément le rôle de ces derniers, la Commission a noté l'existence de dispositions antinomiques ne permettant pas de déterminer s'ils délivreront des identités numériques selon des modalités techniques leur demeurant propres eu égard aux niveaux de sécurité exigés par l'Etat ou s'ils n'agiront que comme intermédiaires concourant à l'enrôlement de l'identité numérique délivrée par l'Etat.

La Commission a également identifié, des échanges survenus entre son Secrétariat Général et la Délégation Interministérielle chargée de la Transition Numérique, d'éventuelles difficultés techniques liées au processus de création de l'identifiant numérique constitutif de l'identité numérique. Or, comme elle l'a rappelé, la fiabilité du dispositif repose sur la qualité de l'identification des personnes.

Sur le consentement

En écho à l'article 5 de la Loi n° 1.483 qui dispose qu'une identité numérique est « *créée et attribuée à toute personne physique ou morale enregistrée dans un registre d'un service public, tenu pour application d'une disposition législative ou règlementaire dont la liste est publiée par Ordonnance Souveraine* », la Commission s'est inquiétée de l'automaticité de la création et de l'attribution d'une identité numérique dès lors qu'un registre sera intégré à la liste publiée par Ordonnance Souveraine. Elle a ainsi souligné que cette attribution s'effectuera sans que les personnes concernées y consentent ou en soient informées.

En outre, la Commission s'est interrogée sur la possibilité qu'un Service ou établissement public bénéficie de la qualité de fournisseur d'identité compte tenu du lourd régime de responsabilité associé.

Concernant les modalités d'accès des personnes aux informations les concernant contenues dans le registre, il lui a semblé, de manière regrettable, que celui-ci ne pourrait s'effectuer que par le biais du kiosque.

Enfin, la Commission a souhaité mettre en parallèle le principe du « *dites-le nous une fois* », qui, en vertu de la Loi sur la Principauté numérique (art. 50), permet aux Services de l'Administration, sous réserve du consentement de l'administré, d'utiliser les informations nominatives, strictement nécessaires, le concernant, obtenues auprès d'un seul d'entre eux avec l'article 13 alinéa 3 de la Loi n° 1.483 qui dispose que « *(...) le service chargé de la gestion du RNMIN peut communiquer au requérant d'autres données que celles qui ont été déterminées en application de l'alinéa précédent, dès lors que la personne concernée y a préalablement consenti de façon expresse* ».

La Commission a été interpellée par ce consentement non défini par la Loi n° 1.483. Il lui a été indiqué que des précisions étaient apportées par l'article 7 du projet d'Ordonnance Souveraine portant application des articles 6, 8 et 13 de la Loi n° 1.483 et que la notion de fournisseur de

données qui est y mentionnée a pour but de viser les « *fichiers sources* » des traitements interconnectés avec le RNMIN.

La Commission a néanmoins regretté qu'aucune précision ne soit apportée par l'Ordonnance Souveraine sur la nature du consentement, sa portée, sa temporalité, ce qui, d'après elle, pourrait laisser à penser qu'une fois *« un consentement obtenu »*, les données des fichiers sources pourraient être accessibles. De même, elle a estimé qu'on pourrait y voir l'existence d'un lien technique direct entre le traitement du fournisseur de service et le traitement du fournisseur de données, dont le rôle exact reste par ailleurs à définir.

Sur les points spécifiques aux différents projets d'Ordonnances Souveraines

- **Le projet d'Ordonnance Souveraine portant application des articles 4 et 5 de la Loi n° 1.483**

La CCIN a compris, après les explications qui lui ont été apportées par les Services Exécutifs de l'Etat, que la connexion à un service en ligne permettra à un fournisseur de faire le lien entre l'identité numérique d'une personne et son possible identifiant client s'il en détient déjà un.

Elle a fait observer que ce lien entre identité numérique et identifiant client ne pourrait se faire ni sur le support de l'identité numérique, ni sur le RNMIN mais uniquement chez le fournisseur de service qui le désire.

Aussi la CCIN a suggéré que le dernier alinéa de l'article 1er du projet d'Ordonnance Souveraine soit supprimé afin d'éviter d'être interprété comme permettant à d'autres identifiants d'être enregistrés dans le RNMIN ou sur le support de l'identité numérique.

Elle avait, de plus, retenu, des explications fournies par les Services de l'Etat, que l'Ordonnance Souveraine disposerait qu'un niveau de garantie d'une identité numérique permette d'accéder aux services d'un niveau moindre. Elle estime qu'il aurait pu être opportun d'y préciser, par la même occasion, à qui incombe la décision de demander un niveau de garantie pour accéder à un service.

- **Le projet d'Ordonnance Souveraine portant application des articles 6, 8 et 13 de la Loi n° 1.483**

La Commission a relevé, des dispositions du projet d'Ordonnance Souveraine, que le RNMIN « *constitue une base de données participant notamment à la production de documents d'identité et à tout autre document administratif, quel qu'en soit le support* ».

Elle a cependant souligné que les documents d'identité sont constitués à partir de traitements métiers et non à partir des informations du Registre qui ne fait qu'alimenter la délivrance de l'identité numérique sur le support de la carte d'identité pour les seules personnes désirant activer leur certificat.

La participation susvisée est, pour la CCIN, davantage liée à l'interconnexion avec le service de confiance visé à l'article 5 de la Loi n° 1.483, laquelle est, selon elle, constitutive d'interrogation sur les choix opérés de l'identité numérique monégasque.

S'agissant des requêtes pouvant être effectuées, en vertu de l'article 13 de la Loi n° 1.483, par les services publics et personnes du secteur privé, auprès du Service en charge du RNMIN, la Commission a noté qu'aucune précision n'est donnée quant à leur objectif ou leurs limites.

Enfin, elle a mis en avant la nécessité qu'un éclaircissement soit apporté sur les rapports et les rôles entre le RNMIN et les acteurs privés dont elle comprend qu'ils sont d'ores et déjà visés par les textes pour répondre à une philosophie d'identité numérique pour tous, et pas uniquement régalienne.

- **Le projet d'Ordonnance Souveraine portant application des articles 17 et 18 de la Loi n° 1.483**

La Commission a relevé, qu'en étant érigé en service de confiance, certaines des obligations auxquelles devrait se soumettre le fournisseur d'identité, en vertu du projet d'Ordonnance Souveraine, lui sont en réalité déjà applicables en application de la Loi pour une Principauté Numérique.

Elle avait par ailleurs été interpellée par la notion de « *moyen d'authentification* » introduite, pour la première fois, à l'article 5 de l'Ordonnance Souveraine projetée, sans y être définie. A cet égard, elle a pris bonne note que ce terme serait remplacé, dans la version finalisée du texte, par celui de « *moyen d'identification* ».

Eu égard aux interrogations passées des Services du Gouvernement pour exiger la conservation, dans certains domaines sensibles, des données personnelles en Principauté, la Commission a estimé que l'identité numérique pourrait nécessiter d'imposer un tel hébergement.

Enfin, elle a constaté que rien ne permet à un fournisseur d'identité de demander d'autres informations que celles prévues au Registre et dont il aurait pu avoir besoin pour la délivrance de ses services en ligne.

La CCIN s'est aussi prononcée, de manière concomitante, sur deux projets d'Ordonnances Souveraines destinées à encadrer les modalités de délivrance de la carte d'identité monégasque et de la carte de résident ayant vocation à pouvoir servir de support physique à l'identité numérique des nationaux et des résidents, ainsi que sur un projet d'Arrêté Ministériel y afférent.

Avis sur un projet d'Ordonnance Souveraine relative à la carte d'identité monégasque et sur un projet d'Ordonnance Souveraine portant modification de l'Ordonnance Souveraine n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté et son Arrêté Ministériel portant application de l'article 4.

La Commission n'a, en premier lieu, pas manqué de relever que les titres régaliens seront désormais, tous deux, munis d'une mémoire électronique. Si les cartes d'identité en étaient déjà dotées, la Commission a constaté un enrichissement de la mémoire électronique par « *les moyens d'utilisation de l'identité numérique* », « *les clés privées de chiffrement relatives aux moyens visés au chiffre 1°* » et « *le prestataire de service de confiance qui délivre les moyens visés au chiffre 1°* ». Elle a, de ce fait, fortement regretté l'absence de définition des « moyens d'utilisation de l'identité numérique » et s'est interrogée sur la notion de « *prestataire de service de confiance* ».

Par ailleurs, elle a constaté, à la lumière des textes projetés, un possible accès aux éléments inscrits dans la mémoire électronique des titres d'identité et de séjour « au travers des technologies de connexion avec et sans contact ». Aussi, bien qu'il lui ait été indiqué que les interconnexions et interopérabilités prévues ne le seront qu'avec d'autres fichiers des Services Exécutifs de l'Etat en lien avec l'identité numérique, la Commission a néanmoins souligné que la question d'une éventuelle lecture autonome des éléments contenus dans la mémoire électronique des titres par d'autres Services ou en lien avec les autorisations prévues par la Loi n° 1.483 relative à l'identité numérique n'était pas pour autant caduque.

En outre, elle a déploré qu'aucune d'alternative au kiosque ne soit prévue pour renouveler les certificats électroniques ce qui, selon elle, pourrait dissuader voire empêcher certains de procéder à ce renouvellement. De même, elle a constaté que l'activation et le renouvellement des certificats par ce biais reposent sur un dispositif biométrique de reconnaissance faciale et a rappelé la nécessité de s'assurer du consentement libre et éclairé des personnes concernées.

Pour ce qui est des conditions de renouvellement des certificats, qui sont dotés d'une durée de vie de 3 ans, la Commission a constaté qu'ils sont déposés par défaut lors de la création d'un titre, charge aux personnes de les activer dans les délais. Elle notait, à cet égard, que la période de jouissance des certificats est d'autant plus brève que les personnes tardent à les activer et s'interrogeait sur l'exigence de renouvellement des clés privées de chiffrement et des certificats électroniques associés à l'identité numérique avant leur date de fin de validité.

S'agissant du projet d'Ordonnance Souveraine portant modification de l'Ordonnance Souveraine relative aux conditions d'entrée et de séjour des étrangers dans la Principauté et son Arrêté

Ministériel portant application de l'article 4, la Commission a relevé une incohérence résultant d'une divergence entre l'âge de délivrance de la carte de séjour tel que prévu dans le projet d'Arrêté Ministériel et celui fixé par l'Ordonnance Souveraine n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté. La Commission a pris acte qu'une modification de l'Ordonnance Souveraine susvisée devrait intervenir sans qu'une date précise ne lui ait été communiquée.

En outre, la Commission a discuté le choix de recourir à un Arrêté Ministériel alors que l'identité numérique dérivée de la carte d'identité est encadrée par une Ordonnance Souveraine, notamment eu égard à la hiérarchie des normes. De plus, elle a estimé que le recours à un Arrêté Ministériel pour encadrer une collecte de données biométriques est un véhicule juridique trop faible. La Commission a toutefois cru comprendre des explications des Services gouvernementaux que le choix de recourir à un Arrêté Ministériel serait lié à de futures modifications apportées à l'Ordonnance Souveraine n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté.

Enfin, bien qu'elle ait pris acte de la volonté du Gouvernement de restreindre les interconnexions avec les fichiers des Services Exécutifs de l'Etat à celles en lien avec l'identité numérique, la Commission a relevé qu'il aurait été préférable de déterminer les finalités et flux de communication envisagés.

LES TRAITEMENTS DE DONNÉES EN LIEN AVEC L'IDENTITÉ NUMÉRIQUE

Parallèlement à l'avis rendu sur les projets d'Ordonnances Souveraines relatives à l'identité numérique , la CCIN s'est prononcée sur plusieurs demandes d'avis portant sur les traitements en lien avec l'identité numérique, ainsi que deux téléservices, relatifs respectivement à :

- la gestion des opérations nécessaires à l'établissement et à la délivrance de la Carte d'Identité Monégasque ;
- la gestion des identités numériques au travers du Registre National Monégasque de l'Identité Numérique, dénommé RNMIN ;
- la gestion des moyens d'utilisation de l'identité numérique inscrits sur les cartes d'identité monégasque et les cartes de séjour (certificats, code CAN et PUK), dénommé CLCM ;
- la fourniture des services de confiance pour l'identité numérique, dénommé MConnect et MConnect Mobile ;
- la plateforme d'activation et de gestion de l'identité numérique après délivrance du titre, dénommé Kiosque ;
- l'utilisation de l'identité numérique des monégasques et résidents par le biais d'une application mobile dédiée, dénommé MConnect Mobile.

Les nouveaux traitements liés à l'implémentation de l'identité numérique

La Commission a tenu à rappeler, à travers ses divers avis, que les Ordonnances Souveraines servant de base légale aux traitements liés à l'identité numérique devront être publiées, au plus tard, concomitamment à la mise en œuvre des traitements associés.

Pareillement, elle a estimé, concernant l'information des personnes concernées, que l'existence de l'ensemble des traitements découlant de l'identité numérique[2] doit être portée à leur connaissance lors de la remise de leur titre (carte d'identité ou de séjour) et que les interconnexions ne peuvent être effectuées qu'entre des traitements légalement mis en œuvre.

En outre, elle a formulé un certain nombre de remarques spécifiques à chaque traitement.

La « *Gestion des opérations nécessaires à l'établissement et à la délivrance de la carte d'identité Monégasque* »

Dans la perspective de la délivrance de nouvelles cartes d'identité répondant à de nouveaux besoins de renforcement des dispositifs de sécurité et destinées à devenir le support de l'identité numérique des nationaux, la Commission a substitué la délibération portant la référence 2021-108 à celle initialement rendue le 2 mars 2009.

A cet égard, elle a notamment exprimé son inquiétude quant à l'incertitude pesant sur la définition exacte du rôle de la Mairie résultant des différents textes, à savoir Autorité d'enregistrement de l'identité légalement définie par l'Ordonnance Souveraine projetée relative à la carte d'identité monégasque ou alors, fournisseur d'identité au sens des articles 1er, 17 et 18 de la Loi n° 1.483 relative à l'identité numérique ce qui lui confèrerait la qualité de service de confiance au sens de la Loi n° 1.383 pour une Principauté numérique.

La Commission a par ailleurs relevé la collecte de divers formulaires, mais aussi de certificats médicaux ouvrant droit à un enrôlement au domicile de la personne concernée ou attestant de son incapacité de signer. Sans qu'elle considère ces informations excessives au regard de la finalité du traitement, la Commission a néanmoins fixé la durée de conservation des formulaires à la durée de validité de la carte. Elle a également demandé à ce que la photographie collectée dans le cadre de ce traitement soit supprimée dès l'enrôlement sur la mémoire électronique de la carte d'identité monégasque comme cela était jusqu'à présent le cas.

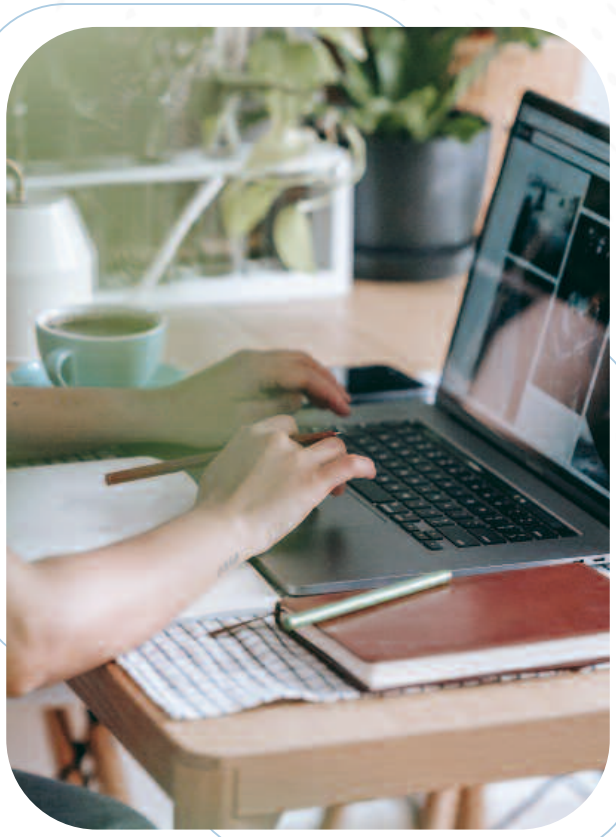
En termes de sécurité elle a rappelé l'importance de veiller régulièrement à la sécurité du poste mobile permettant l'enrôlement au domicile des personnes.

La « Gestion des identités numériques au travers du Registre National Monégasque de l'Identité Numérique »

Concernant le traitement du Registre National Monégasque de l'Identité Numérique (le « *RNMIN* »), qui a notamment pour objet d'identifier des personnes physiques ou morales avec l'attribution d'un identifiant numérique lié à une identité numérique, la Commission a, tout d'abord, constaté que les personnes présentées comme concernées par le traitement regroupent celles qui l'étaient au jour de la présentation de la demande d'avis.

Aussi, elle a souhaité rappeler que ce registre pourrait, également, en vertu de l'article 5 de la Loi sur l'identité numérique, concerner d'autres catégories de personnes et que leur adjonction nécessitera que des modifications soient apportées au présent traitement. La Commission a considéré

[7] Voir supra



que ces modifications devront clarifier le rôle des fournisseurs d'identité et ses conséquences sur les personnes concernées.

Enfin, elle a estimé, en l'absence de définition des missions du service en charge du RNMIN et de précisions relatives à son Autorité de rattachement, qu'une Ordonnance Souveraine devrait être publiée pour en préciser le fonctionnement effectif.

La « *Gestion des moyens d'utilisation de l'identité numérique inscrits sur les cartes d'identité monégasque et les cartes de séjour (certificats, code CAN et PUK)* »

Dans le prolongement de son avis sur le RNMIN, la Commission s'est prononcée sur son « extension technique », soulignant notamment les difficultés juridiques et techniques générées par la distinction, non nécessaire, faite entre ces traitements. Elle a constaté que cette dissociation théorique entraine des incohérences dans les interconnexions légalement prévues. La Commission a demandé à ce que des clarifications soient apportées sur l'autonomie du traitement mais aussi, sur les définitions légales des « *moyens d'utilisation de l'identité numérique* » et sur la cohérence de la présence de certificats de signature électronique sur l'extension technique du registre, lequel n'est pas limité aux seuls résidents et nationaux mais concerne in fine toute personne inscrite par un fournisseur d'identité public ou privé.

La « *Fourniture des services de confiance pour l'identité numérique* »

Une nouvelle fois, la Commission a tenu à rappeler qu'une identité numérique pourra être délivrée par un fournisseur d'identité à toute personne inscrite dans un registre tenu par un Service Public ou dans un fichier d'un fournisseur d'identité privé. Or, les modalités de délivrance de l'identité numérique, par ces fournisseurs, ne sont pas définies, à ce-jour, de sorte que la Commission a indiqué ne pas être en mesure de déterminer leur degré d'autonomie pour la délivrance de certificats d'authentification.

Au titre des fonctionnalités du traitement trois « services » authentification, signature et dérivation mobile de l'identité numérique ont été présentés, à la Commission, comme étant interconnectés avec le RNMIN. La Commission a souligné à cet égard que seul un service de confiance d'identification et d'authentification est légalement consacré dans la Loi sur l'identité numérique, ses projets de textes d'application et les Ordonnances Souveraines sur la carte d'identité et les titres de séjour pour être interconnecté avec le RNMIN. De surcroît, il lui a semblé que les services de signature et de dérivation sont dédiés uniquement aux monégasques et résidents et non à l'ensemble des personnes devant, à terme, figurer dans le Registre.

En tout état de cause, compte-tenu des spécificités relevées concernant le service de dérivation mobile de l'identité numérique « *MConnect Mobile* », la Commission a estimé qu'il devait faire l'objet d'une formalité dédiée et répondre à ses interrogations juridiques et techniques. Elle a donc demandé que ce service ne soit pas activé avant qu'une telle formalité ne lui ait été soumise.

Cette formalité ayant pour finalité « *Permettre l'utilisation de l'identité numérique des monégasques et résidents par le biais d'une application mobile dédiée* » lui a été présentée et a obtenu un avis favorable de la Commission.

La Commission s'est enfin inquiétée de la faisabilité technique de l'ouverture d'une identité numérique aux autres populations visées par la Loi n° 1.483 relative à l'identité numérique tant le traitement qui lui a été soumis lui est apparu comme ayant été réfléchi pour la fourniture d'une identité régalienne.

Elle a observé que ce traitement serait interconnecté avec deux premiers téléservices nécessitant une authentification d'un niveau de garantie élevée, ayant pour finalité respective :

- « *Réaliser une déclaration sur l'honneur par le biais d'une démarche en ligne* » ;
- « *Réaliser une signature entre plusieurs parties par le biais d'une démarche en ligne* ».

Ces derniers ont obtenu un avis favorable de la Commission.

La « *Plateforme d'activation et de gestion de l'identité numérique après délivrance du titre* »

Il a été prévu que l'activation des certificats d'authentification, pour ceux ne l'ayant pas été lors de la délivrance du titre, s'effectue par le biais d'un kiosque.

La Commission a demandé que les personnes concernées soient, a minima, informées directement sur le kiosque de leurs droits au titre de l'article 14 de la Loi n° 1.165 relative à la protection des informations nominatives et du recours à un dispositif de reconnaissance faciale.

En effet, il est apparu que la mention d'information, accessible depuis le kiosque, renvoie les explications à un URL ou un QR code. La Commission a estimé que cette solution n'était pas satisfaisante en ce qu'elle conditionne l'accès aux informations à la détention d'un téléphone et à la réalisation d'une manipulation pour accéder au site du Gouvernement.

Concernant le recours au dispositif de reconnaissance faciale embarqué dans le kiosque, elle a également demandé qu'une alternative au recours au dispositif biométrique soit mise en place dans les meilleurs délais afin de laisser un libre choix aux personnes concernées de recourir ou non à de la biométrie.

Les modifications apportées à des traitements existants

Des demandes modificatives de traitements impactés par les évolutions liées à l'identité numérique ont également été adressées à la Commission.

Le fichier des Nationaux et de leur famille

La Commission a été saisie d'une demande d'avis modificative liée à la création d'une interconnexion entre le traitement concernant le « *Fichier des Nationaux et de leur famille* » et celui du RNMIN afin de permettre la création et l'inscription des Nationaux au Registre.

A titre liminaire, elle a relevé l'existence d'un rapprochement entre le traitement relatif au sommier de la nationalité et le traitement relatif au fichier des nationaux, dès lors qu'une personne inscrite au sommier l'est dans le fichier des nationaux.

Les informations relatives aux Nationaux et nécessaires au RNMIN ayant été listées à l'article 4 du projet d'Ordonnance Souveraine portant application de plusieurs articles de la Loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique, la Commission a observé que l'interconnexion nécessite une collecte supplémentaire de données dans le traitement du Fichier des Nationaux. Il est également apparu un rapprochement avec le traitement, légalement mis en œuvre « *Gestion de la communication électronique* ».

La gestion et le suivi des conditions d'entrée et de séjour des résidents étrangers de la Principauté

De manière parallèle, la Direction de la Sûreté Publique (DSP) lui a adressé une demande modificative liée au traitement de suivi des conditions d'entrée et de séjour des résidents étrangers de la Principauté. Celle-ci avait notamment pour objet de rajouter des interconnexions entre le traitement susvisé et les téléservices permettant de réaliser toutes démarches en ligne concernant la gestion de cartes de séjour ainsi qu'avec la plateforme nécessaire à la délivrance et la gestion des cartes de séjour dans le cadre de l'identité numérique.

Si la Commission a considéré que l'interconnexion avec les téléservices était légitime, elle a toutefois tenu à rappeler que ces derniers devront en amont être légalement mis en œuvre.

La Commission avait, par ailleurs, constaté que des communications de données au Service des Titres et de la Circulation pouvaient être effectuées. Aussi, elle a rappelé, qu'elle s'était d'ores et déjà interrogée sur les raisons de telles communications et avait demandé, dans le cadre d'une délibération passée, qu'il y soit mis fin.

Elle a réitéré sa demande, tout en soulignant une contradiction avec le principe du « *dites-le nous une fois* », lequel repose sur le consentement préalable des personnes.

La plateforme permettant la délivrance et la gestion des cartes de séjour

Enfin, la Commission s'est prononcée sur la demande d'avis modificative liée à la plateforme permettant la délivrance et la gestion des cartes de séjour et s'est inquiétée de l'incertitude pesant sur la définition exacte du rôle de la DSP, liée à la multitude de textes auxquels il était fait référence pour justifier le traitement.

Elle a rappelé que l'éventuelle qualification de la DSP, en fournisseur d'identité, emporte des conséquences juridiques non mentionnées au dossier.

En outre, concernant l'information préalable, la Commission a notamment demandé que les personnes concernées soient directement informées de leurs droits, en application de l'article 14 de la Loi n° 1.165 et de la transmission de leurs informations aux différents traitements permettant la délivrance de l'identité numérique.

En toute fin, en matière de sécurité, elle a rappelé que la sécurité du poste mobile, utilisé pour enrôler les identités numériques des résidents attestant d'une incapacité à se rendre dans les locaux de la DSP ou à signer, doit être vérifiée régulièrement.

07

LES DOSSIERS DU SECTEUR PUBLIC ET ASSIMILÉ

LA GESTION DES AUTORISATIONS D'EXERCER DES PROFESSIONNELS DE SANTÉ

Par délibération n° 2021-050 du 17 mars 2021, la Commission a émis un avis favorable à la mise en œuvre par la Direction de l'Action Sanitaire (DASA) d'un traitement ayant pour finalité « *Gestion des autorisations d'exercer des professionnels de santé* ».

Celui-ci permet à un professionnel de santé ou assimilé d'adresser par voie postale ou électronique sa demande d'autorisation d'exercice en Principauté. Ce dossier comprend entre autres un extrait de casier judiciaire de moins de trois mois, une copie d'une pièce d'identité, titre de séjour ou passeport, les diplômes, une notice de renseignements.

La DASA transmet alors par courrier à la Sûreté Publique pour « enquête habituelle » la notice de renseignements accompagnée de l'extrait de casier judiciaire daté de moins de trois mois et de la copie de la pièce d'identité ou du passeport.

En outre, suivant la profession, l'instance ou l'association professionnelle concernée est consultée pour avis.

La DASA réceptionne ensuite les avis de la Sûreté Publique et de l'instance ou de l'association professionnelle concernée et transmet un projet de délibération et d'Arrêté Ministériel au Département des Affaires Sociales et de la Santé (DASS) afin que la demande d'autorisation soit examinée en Conseil de Gouvernement.

Des autorisations permanentes ou ponctuelles sont ainsi délivrées.

La Commission a cependant demandé que les accès effectués aux applications métiers et bases courriers par la DSI ainsi que les sauvegardes de ces accès soient collectés et qu'un message/une alerte soit envoyé(e) au responsable métier l'informant de cet accès qui sera préalablement justifié ou devra l'être.

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

La Commission a par ailleurs fixé la durée de conservation des logs de connexion à 1 an et celle des candidatures non retenues à 5 ans.

Enfin, elle a demandé que l'extrait de casier judiciaire soit supprimé dès le retour de la Direction de la Sûreté Publique.

Les projets e-santé portés par le Département des Affaires Sociales et de la Santé

Le système médical monégasque est en train d'opérer sa transformation numérique afin d'offrir aux patients une santé connectée. C'est dans ce contexte que 3 importants traitements automatisés de données concernant la prise en charge des patients en Principauté ont été soumis à la Commission pour avis par le Département des

Affaires Sociales et de la Santé (DASS), en collaboration avec la Délégation Interministérielle pour la Transition Numérique.

La messagerie sécurisée pour les échanges de données de santé

Par délibération n° 2021-159 du 21 juillet 2021, la Commission s'est prononcée favorablement au traitement ayant pour finalité « *Echange de données de santé à travers un système de messagerie sécurisée* ».

Comme l'a indiqué le responsable de traitement, ce système qui concerne les professionnels de santé et les patients qu'ils prennent en charge « *repose sur le principe de fonctionnement d'un coffre-fort. Le professionnel habilité rédige un message incluant ou non des pièces jointes à partir d'une boîte mail sécurisée et à destination d'un/plusieurs professionnel(s) habilité(s). Le message et les données sont stockés dans un coffre-fort et mis à disposition du destinataire. Le destinataire est prévenu de la mise à disposition de ce message et doit se connecter au serveur de messagerie pour récupérer le message de manière sécurisée* ».

Si elle a pris acte que les accès du personnel du prestataire en charge de l'infogérance étaient tracés, la Commission a toutefois demandé que les professionnels de santé habilités soient informés de ces potentiels accès.

Le Portail de e-santé « MonacoSanté »

Afin de gérer un portefeuille de services numériques à destination des patients (usagers) et des professionnels de santé autorisés à exercer en Principauté, le Gouvernement Princier a mis en place un portail de e-Santé, exploité par le Département des Affaires Sociales et de la Santé (DASS).

En 2019, la Commission avait émis un avis favorable à la mise en œuvre de ce traitement par délibération n° 2019-169 du 20 novembre 2019 mais les modalités d'exploitation de ce portail ayant évolué, le responsable de traitement a donc souhaité remplacer le traitement initial par un nouveau traitement qui a lui aussi fait l'objet d'un avis favorable de la Commission par délibération n° 2021-221 du 20 octobre 2021.

A son ouverture, la plateforme comprendra les fonctionnalités principales suivantes :

- gestion d'un annuaire en ligne de tous les professionnels de santé autorisés à exercer à Monaco ;
- gestion d'un service de prise de rendez-vous en ligne sur des créneaux spécifiques et déterminés par le professionnel de santé, notamment à des fins de vaccination contre la Covid-19 ;

- gestion d'un service d'actualités de santé à destination du grand public et des professionnels de santé ;
- gestion d'un forum d'échange avec modérateur entre les professionnels de santé uniquement et le Gouvernement de Monaco ;
- gestion des comptes utilisateurs (patients et professionnels de santé) ;
- gestion des habilitations (matrice des droits, gestion et création des profils, audit trail) ;
- établissement de statistiques (tableau de bord, reporting).

Concernant le forum d'échange, la Commission a pris acte des précisions du responsable de traitement selon lesquelles ledit forum « *permettra aux professionnels de santé uniquement (pas aux patients ni aux visiteurs) d'interagir avec le Gouvernement de Monaco (utilisateurs ayant les droits d'Administration sur le portail) sur des sujets en lien avec le projet de e-Santé de la Principauté* ».

Par la suite, la plateforme s'enrichira des fonctionnalités suivantes :

- fourniture d'une application mobile pour les patients :
- annuaire et prise de rendez-vous ;
- numéros d'urgence ;
- authentification (avec une limitation pour les seuls utilisateurs « *Patients* ») ;
- gestion des cookies ;
- accès aux « *Mentions Légales* » et aux « *Conditions générales d'utilisation* » ;
- création d'un cookie pour déclarer le contexte d'exécution ;
- restriction des droits utilisateurs pour se connecter à l'application (seuls les patients sont autorisés à se connecter) ;
- gestion d'une messagerie sécurisée de santé ;
- gestion d'une solution de téléconsultation ;

- gestion de la migration des agendas des professionnels de santé papier ou numérique vers l'agenda du portail MonacoSanté ;
- gestion de l'envoi d'une campagne de SMS automatiques aux patients des professionnels de santé ayant migré leur agenda ;
- gestion d'un service de notifications permettant d'afficher sur la page principale du portail une pastille indiquant le nombre de notifications, c'est-à-dire le nombre de nouvelles informations à disposition de l'utilisateur.

S'agissant plus spécifiquement de la migration des agendas des professionnels de santé, la Commission a souligné qu'afin de préserver le secret médical, cette migration serait effectuée par l'intermédiaire d'un médecin mandaté par le Gouvernement.

Concernant les moyens de paiement acceptés, le responsable de traitement a indiqué qu'« *aucun règlement ne s'effectue via le portail en ligne* » et qu'il n'y a « *aucune récupération de données bancaires* ».

La Commission a en outre précisé que tout rapprochement et interconnexion avec d'autres traitements devait être effectué avec des traitements légalement mis en œuvre.

La mise en place de la téléconsultation

Cette année, le Gouvernement Princier a également souhaité mettre en place un service de consultation à distance nommé « *téléconsultation* » entre le professionnel de santé utilisateur du portail MonacoSanté et son patient.

Les fonctionnalités de ce traitement sont les suivantes :

➢ Pour les professionnels de santé :

- gérer les téléconsultations programmées ;
- consulter le télédossier du patient et déposer les ordonnances et comptes-rendus ;
- facturer une téléconsultation ;
- gérer le paiement des téléconsultations ;
- envoyer au patient un email lors de la création du rendez-vous en téléconsultation ;
- envoyer au patient un email et un SMS lors de la création du télédossier ;
- scanner sa signature qui sera opposable sur les documents transmis au patient (enregistrée sur l'espace de téléconsultation du professionnel de santé) ;
- fournir les documents nécessaires à son identification ;
- télécharger un récapitulatif mensuel de ses téléconsultations.

➢ Pour les patients :

- prendre un rendez-vous en téléconsultation ;
- être informé par email du lien d'accès à l'espace de téléconsultation ;
- tester son matériel ;
- prépayer sa téléconsultation ;
- accéder à la salle d'attente virtuelle ;
- être informé d'un retard (action manuelle du professionnel de santé) ;
- être appelé par le professionnel de santé ;
- accéder directement à la visio-conférence ;
- être alerté par SMS que le professionnel de santé l'appelle et que le patient n'est pas connecté ;
- télécharger des documents (compte-rendu de consultation, ordonnance) ;
- payer la consultation après le rendez-vous ;
- accéder à l'assistance de la téléconsultation ;
- valider les Conditions Générales d'Utilisation (CGU).

Par délibération n° 2021-222 du 20 octobre 2021, la Commission a émis un avis favorable, sous réserve toutefois de la prise en compte de ses observations.

C'est ainsi que pour l'exercice du droit d'accès, elle a constaté à la lecture des pièces jointes au dossier, qu'« *un justificatif d'identité, en noir et blanc, pourra être demandé au requérant* ».

A ce titre, la Commission a précisé que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Elle a par ailleurs rappelé que le droit d'accès aux données de santé par les patients ne peut s'effectuer que directement sur la plateforme ou auprès des professionnels de santé concernés.

LA POURSUITE DU DÉVELOPPEMENT DES DÉMARCHES EN LIGNE

Comme chaque année maintenant, la Commission a examiné en 2021 de nombreuses demandes d'avis relatives à des téléservices mis en œuvre par l'Administration afin de faciliter les démarches des usagers.

Tel a été notamment les cas d'un traitement exploité par la Direction de l'Environnement, visant à dématérialiser certaines démarches au bénéfice des usagers par le biais d'un nouveau téléservice. L'objectif de ce traitement est de permettre aux demandeurs d'effectuer leurs demandes en ligne sans se déplacer ; d'être notifiés et de suivre l'avancement de leurs demandes ; de télécharger les justificatifs et décisions émises par l'Administration, et à l'Administration d'obtenir des statistiques sur les demandes effectuées ; de simplifier le travail des agents traitants en automatisant certaines actions ; de faciliter le suivi des dossiers par les agents traitants grâce aux outils de recherche et aux historiques des demandes.

Il en a été de même concernant la dématérialisation des relations entre les locataires et occupants avec l'Administration des Domaines dont l'objet est de proposer aux occupants de locaux domaniaux une gestion dématérialisée des échanges avec l'Administration par le biais d'un extranet permettant plusieurs fonctionnalités, telles que la gestion des comptes utilisateurs, le paiement en ligne des loyers ou la consultation de documents en ligne (loyers, baux, quittances, etc.). Composé d'un site web et d'une application mobile permettant aux locataires de visualiser les dernières informations de leur compte vis-à-vis de l'Administration des Domaines, il vise à faciliter les démarches des occupants de logements domaniaux.

La Direction de l'Education Nationale de la Jeunesse et des Sports (DENJS) a déployé également de nombreux téléservices 2021, que ce soit en matière d'inscription dans certaines filières d'études, d'inscription scolaire, y compris en dehors des périodes d'inscriptions traditionnelles, de demandes d'autorisation d'absence exceptionnelle, ...

Consciente de l'intérêt qui s'attache à proposer cette dématérialisation, la Commission rappelle cependant de manière systématique qu'en application des dispositions de l'article 42 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré « *(...) la création d'un téléservice ne saurait toutefois avoir pour effet de supprimer la possibilité pour l'usager d'accomplir les démarches, formalités ou paiements qui en sont l'objet par des voies autres qu'électroniques* ». Aussi la voie dématérialisée ne doit pas être exclusive, et des alternatives doivent être possibles pour les usagers.

Elle veille également au quantum des informations collectées, qui doivent être en adéquation avec les finalités spécifiques des téléservices, lesquels sont à distinguer des traitements métiers mis en œuvre par les Directions opérationnelles.

En outre, constatant que de plus en plus de traitements métiers ou de téléservices font l'objet d'interventions de Directions supports, ou de tiers intervenants pour leur compte, qui administrent ou créent les solutions (Direction des Systèmes d'Information, Direction des Services Numériques notamment), la Commission souligne que ces Directions ne doivent pas avoir accès en continu aux données nominatives, mais uniquement en cas de besoin d'intervention.

LES TRAITEMENTS DU CENTRE HOSPITALIER PRINCESSES GRACE

Cette année, la Commission a émis 3 avis favorables concernant des traitements mis en œuvre par le Centre Hospitalier Princesse Grace (CHPG).

L'accès au parking par reconnaissance des plaques d'immatriculation

Le 19 mai 2021 la Commission a émis un avis favorable à la mise en œuvre par le CHPG d'un traitement automatisé ayant pour finalité « *Gestion des accès au CHPG avec ouverture automatisée par reconnaissance des plaques d'immatriculation* ».

Celui-ci concerne les pompiers et les membres de la Direction disposant d'un véhicule de fonction et « *a pour objectif de simplifier les accès au parking au moyen d'une ouverture/fermeture automatique des barrières sans utilisation du badge ou du support sans contact, par l'installation d'un système de reconnaissance des plaques d'immatriculation* ».

Le nouveau site internet du CHPG

Lors de sa réunion du 15 septembre, la Commission a émis un avis favorable à la mise en ligne du nouveau site internet du CHPG qui, entre autres fonctionnalités, présente les services de l'hôpital, diffuse des informations sur l'actualité de l'établissement, offre un service de paiement en ligne et propose différents formulaires (candidatures, demande de stages, contact).

Elle a toutefois tenu à rappeler que l'information préalable des personnes concernées qui s'effectue par le biais des mentions légales de ce site devait impérativement être conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

La Commission a par ailleurs interdit l'interconnexion avec un autre site internet administré par le Gouvernement Princier tant que ce dernier n'avait pas reçu un avis favorable de sa part.

Enfin, elle a recommandé que la sécurité du « *Captcha* » utilisé dans l'ensemble des formulaires du site soit renforcée.

Le dossier médical du patient informatisé

Par délibération n° 2021-207 du 20 octobre 2021, la Commission a émis un avis favorable à la mise en œuvre du traitement ayant pour finalité « *Dossier médical du patient informatisé* ».

Concernant toutes personnes admises au CHPG, « *Ce traitement permet de collecter et de partager les informations médicales d'un patient afin d'assurer sa prise en charge lors de ses venues au CHPG. Il permet aux équipes médicales et aux soignants d'exercer leurs activités de prévention, de diagnostics et de soins* ».

La Commission a ainsi pris acte que « *Le dossier médical est composé de comptes rendus de séjours, d'observations médicales, de correspondances, d'ordonnances, de certificats médicaux, de prescriptions (médicaments, soins, examens), d'observations médicales des urgences, de comptes rendus d'examens, de résultats de laboratoire, d'allergies, de traitements en cours, de paramètres vitaux, d'informations nécessitant une traçabilité soit à des fins épidémiologiques, de vigilance ou de besoins statistiques tel que celui de la bonne utilisation des équipements ou des moyens* ».

Elle a par ailleurs noté que ce traitement ne concerne que les données médicales du patient et

que le volet administratif du dossier patient fera l'objet d'un autre traitement déclaré ultérieurement, et a relevé que le présent traitement a vocation à terme à remplacer le traitement actuel ayant pour finalité « *Dossier médical du patient informatisé* », légalement mis en œuvre.

S'agissant de l'exercice du droit d'accès, elle a considéré qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Enfin, en ce qui concerne la conservation du dossier médical pendant 30 ans à compter de la dernière visite du patient, la Commission a noté que conformément à l'article 8 de l'Ordonnance 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, celui-ci est conservé pendant une durée de vingt ans à compter de la date du dernier séjour du patient concerné dans l'établissement de santé ou de sa dernière consultation externe en son sein.

Aussi, elle a fixé la durée de conservation du dossier médical du patient à vingt ans à compter de la date du dernier séjour du patient concerné dans l'établissement de santé ou de sa dernière consultation externe en son sein.

LA PROTECTION DES INFORMATIONS NOMINATIVES EN MATIÈRE DE RECHERCHES BIOMÉDICALES ET NON BIOMÉDICALES

Comme chaque année, la Commission a eu à donner son avis sur des recherches médicales menées par des promoteurs étrangers représentés en Principauté par le Centre Hospitalier Princesse Grace. Celles- ci ont été au nombre de 14 dont 12 recherches biomédicales et 2 recherches observationnelles.

Les recherches biomédicales

Indépendamment de deux recherches liées à la crise sanitaire[8], le 20 janvier 2021, la Commission

a émis 1 avis favorable concernant une recherche biomédicale, l'étude « *PRAVAPREV-01* », présentée par l'Institut régional du Cancer de Montpellier (ICM).

Cette recherche doit concerner 400 patientes randomisées au total dont 15 à Monaco, suivies dans le service de radiothérapie du CHPG, et a pour objectif principal d'évaluer l'efficacité de la pravastatine versus placebo sur la survenue d'un grade ≥2 d'une fibrose mammaire chez des patientes atteintes d'un cancer du sein avec un haut risque de survenue d'une fibrose sévère (identifié par le test NovaGray RILA Breast®).

La Commission a constaté que le document d'information indique que « *Le promoteur pourra communiquer des informations personnelles aux agences règlementaires ou à ses partenaires de recherches. Ces personnes, sociétés et agences peuvent être situées dans votre pays, dans d'autres pays de l'Espace économique européen (EEE), aux Etats-Unis et dans d'autres pays à l'extérieur de l'EEE ; Il est possible que certains pays hors de l'EEE n'offrent pas le même niveau de protection de la vie privée que votre pays* ».

[8] Voir supra chapitre dédié à la crise sanitaire Covid-19

Aussi, elle a tenu à rappeler que si un tel transfert vers un pays ne présentant pas un niveau de protection adéquat devait être effectué, la demande objet de son avis favorable devra être modifiée et une demande d'autorisation de transfert devra lui être soumise.

La Commission a en outre demandé que la communication des données pseudonymisées chiffrées et des clés de déchiffrement soit effectuée par deux canaux distincts.

Dans sa délibération n° 2021-026, la Commission a émis un avis favorable à la mise en œuvre de l'étude « *TARGET BP I* » par la société Ablative Solutions, Inc., localisée aux Etats-Unis. Ladite étude comporte deux cohortes successives, la cohorte RCT qui est une étude phase 3 prospective, randomisée, en aveugle, multicentrique, contrôlée par simulation de dénervation rénale, pour l'évaluation de l'efficacité et de la sécurité de la dénervation rénale par neurolyse alcoolique à l'aide du kit Peregrine, et la cohorte de sécurité qui est initiée après la levée d'aveugle de la cohorte RCT, lorsque le dernier patient à l'étude aura passé sa visite de 6 mois, et uniquement si le critère d'efficacité primaire de la cohorte RCT a été atteint.

Cette étude doit se dérouler dans un maximum de 70 centres établis aux Etats-Unis et en Europe. En Principauté de Monaco, elle est réalisée au CHPG sous la responsabilité d'un médecin investigateur exerçant au sein du service de cardiologie. Le responsable de traitement souhaite inclure jusqu'à 300 patients randomisés au total dans chacune des deux cohortes dont 10 à chaque fois à Monaco.

La Commission a pris acte des précisions du responsable de traitement selon lesquelles dans le cadre de cette recherche « *Les données sur la race et l'ethnie sont collectées car le profil tensionnel et la réponse aux antihypertenseurs sont différents en fonction des populations* ».

Elle a cependant demandé que le formulaire de consentement que signe le patient soit modifié conformément à la « *Fiche d'information du patient* » afin d'indiquer qu'en cas de retrait de la recherche, les informations déjà collectées seront conservées afin de ne pas rendre impossible ou d'affecter sérieusement la réalisation des objectifs de la recherche.

A cet égard, la Commission a noté qu'en cas de retrait de l'étude le patient signe également une « *Notification de retrait de l'étude clinique* » dans laquelle il lui est demandé s'il accepte ou refuse

que d'importantes informations de sécurité supplémentaires le concernant soient extraites de son dossier médical et enregistrées dans la base de données clinique pendant la durée de l'étude.

Aussi, elle a demandé que les patients soient préalablement informés de la nature desdites informations.

Enfin, après avoir constaté que seul le formulaire de consentement mentionne la transmission et le traitement des données des patients « *par le promoteur de la recherche ou par les personnes agissant pour son compte, en Europe et aux Etats-Unis* », elle a demandé que la « *Fiche d'information du patient* » qui était silencieuse sur ce point soit complétée pour préciser les modalités de transfert des données vers les Etats-Unis afin de permettre au patient d'y consentir de manière libre et éclairée.

Concomitamment, la Commission a autorisé cinq transferts des informations collectées dans le cadre de cette étude à destination du datamanager en charge de vérifier la cohérence des informations colligées et des prestataires en charge respectivement de l'analyse des données d'enregistrement automatisé de la pression artérielle envoyées par les ARCs du CHPG, de la mise à disposition d'une plateforme électronique, de l'analyse des angiographies scanner et/ou IRM et de l'analyse des échographies, tous situés aux Etats-Unis.

Lors de cette même séance en date du 17 février 2021, la Commission a également émis un avis favorable à la mise en œuvre d'une étude menée par le laboratoire H.A.C. Pharma, localisé en France.

Cette étude dénommée « *FLU HON* » a pour objectif principal d'évaluer l'efficacité d'un traitement de 4 semaines par la fludrocortisone (FLU) à dose stable sur la chute de pression artérielle (PA) systolique après cinq minutes d'orthostatisme actif, chez des patients atteints d'hypotension orthostatique neurogène (HON) symptomatique, malgré un traitement par les mesures non médicamenteuses associées ou non à la midodrine.

En Principauté, elle devrait concerner cinq patients traités au CHPG sous la responsabilité d'un médecin investigateur exerçant au sein du service de cardiologie.

La Commission a rendu deux nouveaux avis favorables le 17 mars 2021. La premier a concerné l'étude « *EYE-PD* » mise en œuvre par l'Association de Recherche Bibliographique et Scientifique pour les Neurosciences (AREBISN), localisée en France, afin d'étudier l'évolution des marqueurs d'oculomotricité avec le temps chez des patients ayant une Maladie de Parkinson Idiopathique (MPI), de stade léger à modéré.

Elle a cependant demandé que le « Consentement éclairé de participation » soit complété, conformément à la « *Notice d'information* », afin d'indiquer que le patient peut signaler au médecin investigateur qu'il ne souhaite pas que les données déjà recueillies soient traitées et analysées mais que le promoteur peut ne pas faire droit à cette demande pour ne pas compromettre gravement la réalisation des objectifs de la recherche.

Dans sa délibération n° 2021-052 concernant l'étude « *DPD MAX* » mise en œuvre par le Centre Antoine Lacassagne, la Commission a demandé

également que le formulaire de consentement soit complété mais cette fois pour indiquer que les patientes peuvent demander à tout moment la destruction de leurs échantillons biologiques.

Elle a rappelé que la communication des données pseudonymisées chiffrées et des clés de déchiffrement doit être effectuée par deux canaux distincts.

Cette étude qui devrait concerner en Principauté 25 patientes atteintes d'un cancer du sein métastatique a pour objectif principal d'analyser l'influence du phénotype DPD, mesuré par l'activité enzymatique lymphocytaire de la DPD, sur la réponse objective à 6 mois d'un traitement par capécitabine en monothérapie,

Le 21 avril 2021, la recherche « *MEDIC-DIVE* » présentée par l'association PHYMAREX – Institut de physiologie et de médecine en milieu maritime et en environnement extrême, localisée en France, a elle aussi reçu un avis favorable de la Commission.

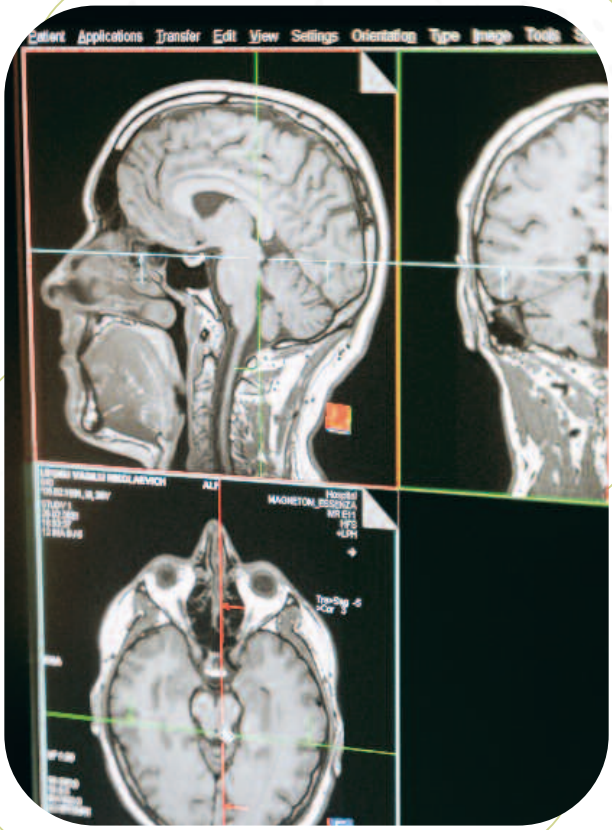
Le responsable de traitement souhaite inclure 60 patients au total dont 30 à Monaco où cette recherche sera réalisée au CHPG sous la responsabilité d'un médecin investigateur exerçant au sein du Service de Médecine d'Urgence.

Cette étude a pour objectif principal d'évaluer l'efficacité de la plongée sous-marine sur les critères de burnout chez les médecins urgentistes. Pour cela, deux stratégies thérapeutiques seront comparées dont l'une inclura la plongée sous-marine.

Le 21 juillet 2021, la Commission s'est également prononcée favorablement à la mise en œuvre par le Centre Hospitalier Universitaire de Nice de l'« *Etude SCHIZOEMP* » qui doit inclure 35 patients au total dont 10 à Monaco, suivis par le Service de psychiatrie.

Cette recherche a pour objectif principal d'identifier des marqueurs électrophysiologiques, issus de la technique des potentiels évoqués cognitifs (ERPs), des différents processus sous tendant le comportement empathique et leurs troubles en psychopathologie contre la schizophrénie.

La Commission a toutefois recommandé que l'ordinateur portable du LAPCOS (Laboratoire d'Anthropologie et de Psychologie Cliniques, Cognitives et Sociales) de l'Université Nice Côte d'Azur soit chiffré.



Le mercredi 20 octobre, l'Etude « *NEWTON AF* » présentée par Boston Scientific S.A. a elle aussi reçu un avis favorable de la Commission.

Cette étude qui doit de dérouler dans environ 50 centres situés en Amérique du Nord, en Asie-Pacifique et en Europe, sera réalisée au CHPG sous la responsabilité d'un médecin investigateur exerçant au sein du Service de cardiologie.

Ladite étude a pour objectif principal d'établir la sécurité et l'efficacité du cathéter StablePoint et du système de détection de force pour le traitement de la fibrillation auriculaire paroxysmique. Outre des données de santé, le responsable de traitement prévoit de collecter également des informations relatives à l'ethnie et la race des patients participant à la recherche.

A cet égard, si la Commission a pris acte des précisions selon lesquelles « *il ne s'agit pas uniquement d'une exigence pour les patients américains, mais globale afin d'examiner les différences épidémiologiques dans le monde entier* », elle a cependant noté que les médecins ont la possibilité de renseigner dans le dossier que la « *race et l'origine ethnique ne sont pas divulgués pour ce sujet* ».

En conséquence, puisque la collecte de ces données est facultative, la Commission a demandé qu'elles ne soient pas collectées en Principauté.

Elle a par ailleurs relevé que le document d'information mentionne que « *L'analyse de l'étude impliquera l'envoi des données à des pays situés en dehors de l'Union européenne (UE) ou de l'Espace économique européen (EEE) où les lois européennes relatives à la protection des données ne s'appliquent pas* » et que le formulaire de consentement que signe chaque patient indique qu' « *il peut être nécessaire de transmettre des données à des pays dans lesquels la législation européenne ou monégasque relative à la protection des données ne s'applique pas (par exemple, les Etats-Unis ou le Japon)* ».

Aussi elle a demandé que les deux documents soient modifiés afin d'indiquer que ces transferts de données se feront vers des destinataires situés aux Etats-Unis afin de permettre au patient d'y consentir de manière libre et éclairée.

En outre, si des transmissions devaient être effectuées vers d'autres destinataires que ceux mentionnés dans la présente demande d'avis, la Commission a rappelé qu'une demande d'avis modificative devra lui être soumise ainsi qu'une ou des demande(s) d'autorisation de transfert si le ou les nouveau(x) destinataire(s) devai(en)t être situé(s) dans un pays ne disposant pas d'un niveau de protection adéquat.

Enfin, elle a autorisé les quatre demandes de transfert à destination des Etats-Unis, soumises concomitamment, vers des prestataires chargés respectivement de l'examen des enregistrements électrocardiographiques, de l'analyse des

données Holter et de stocker, traiter et mettre en œuvre l'automatisation des informations, mais a demandé qu'une demande de transfert complémentaire lui soit soumise dans les plus brefs délais concernant l'archivage des données aux Etats-Unis.

Celle-ci lui a été transmise le 11 novembre et a été autorisée par délibération n° 2021-259 du 17 novembre 2021.

La Commission a par ailleurs émis un avis favorable à la mise en œuvre par le Groupement des Hôpitaux de l'Institut Catholique de Lille d'une recherche dont objectif principal est de comparer l'efficacité du tocilizumab et de l'abatacept par voie sous-cutanée en situation d'échec à une première ligne ou une seconde de traitement ciblé.

Intitulée, « *SUNSTAR* », elle devrait inclure 5 à 10 patients souffrant de polyarthrite rhumatoïde et suivis en Principauté au sein de Service de rhumatologie du CHPG.

Après avoir noté que le document d'information indiquait que les données collectées dans le cadre de cette recherche pouvaient être utilisées pour d'autres projets de recherche dûment autorisés et approuvés par un Comité d'éthique compétent dans le domaine de la rhumatologie, la Commission a relevé que cette utilisation ultérieure des données fait l'objet d'un consentement séparé par le biais de deux cases à cocher au sein du formulaire de consentement, afin que le patient puisse effectivement y consentir ou s'y opposer.

Elle a toutefois rappelé que si ces nouvelles recherches devaient impliquer des accès ou des communications non mentionnés dans la présente demande d'avis, le traitement dont s'agit devra être modifié.

Concernant la sécurité de ce traitement, la Commission a rappelé que les données pseudonymisées extraites sur « *DVD* » ou autre support externe doivent être sécurisées avant toute communication.

Les recherches non biomédicales

Parallèlement à ces recherches biomédicales, deux études observationnelles ont été également soumises à l'avis de la Commission.

C'est ainsi que par délibération n° 2021-153 en date du 21 juillet 2021, celle-ci a émis un avis favorable

à la mise en œuvre de l'observatoire MAJIK, présenté par la Société Française de Rhumatologie, dont l'objectif principal est d'évaluer en vie réelle le maintien thérapeutique des inhibiteurs de JAK à un an chez des patients traités pour un rhumatisme inflammatoire chronique.

Après avoir constaté que le consentement que signe le patient indique que des recherches scientifiques ultérieures pourront être conduites par les chercheurs du promoteur et/ou d'autres partenaires publics ou privés, du territoire national ou international, la Commission a rappelé que si un transfert de données nominatives devait être effectué vers des destinataires non mentionnés dans la présente demande d'avis, ladite demande devra être modifiée. De même, si ce transfert devait s'effectuer vers un pays ne présentant pas un niveau de protection adéquat, une demande de transfert devra lui être soumise.

Enfin, le 15 décembre 2021, lors de sa dernière réunion de l'année, la Commission a émis un avis favorable à la mise en œuvre par Abbvie, localisée en France, d'une étude dont l'objectif principal, chez les patients présentant une polyarthrite rhumatoïde modérée à sévère, est d'évaluer la rémission à 6 mois sous upadacitinib en condition de vie réelle et sur ces patients en rémission à 6 mois, d'évaluer le maintien de la réponse à 12 mois.

Dénommée « *Etude UPHOLD* », elle sera réalisée au CHPG sous la responsabilité d'un médecin investigateur exerçant au sein du Service rhumatologie. 300 patients sont concernés au total dont environ 3 à Monaco.

La Commission a par ailleurs autorisé le transfert soumis concomitamment à destination de la maison mère à des fins d'archivage des données. Elle a demandé que le document d'information soit modifié afin d'indiquer que le transfert des données collectées s'effectue à destination de la maison mère, sise aux Etats-Unis afin de permettre au patient

d'y consentir de manière libre et éclairée, et que le « *Consentement éclairé – Etude non interventionnelle* » que signe le patient soit complété afin d'indiquer le transfert des données à destination de la maison mère.

La Commission a par ailleurs rappelé que si des transmissions de données devaient être effectuées vers des destinataires non mentionnés dans la présente demande d'avis, ladite demande devra être modifiée et que si de telles transmissions devaient être effectuées vers des pays ne disposant pas d'un niveau de protection adéquat, une ou des demande(s) de transfert devra/devront lui être soumise(s).

Concernant la sécurité, elle a rappelé que la communication des données pseudonymisées chiffrées et des clés de déchiffrement doit être effectuée par deux canaux distincts.

08

LES AVIS DE LA COMMISSION SUR LES PROJETS DE TEXTES LÉGISLATIFS OU RÉGLEMENTAIRES

Conformément à l'article 2 alinéa 2 de la Loi n° 1.165 du 23 décembre 1993, « *la Commission est consultée par le Ministre d'Etat lors de l'élaboration de mesures législatives ou règlementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement des informations nominatives et peut l'être pour toute autre mesure susceptible d'affecter lesdits droits et libertés* ».

Indépendamment des saisines relatives à des projets de textes liés à la crise sanitaire et à la mise en œuvre de l'identité numérique[9], la CCIN a été consultée à 2 reprises par le Ministre d'Etat.

L'ORDONNANCE SOUVERAINE N° 8.258 PORTANT APPLICATION DE LA LOI N° 1.491 DU 23 JUIN 2020 RELATIVE AUX OFFRES DE JETONS

Le 16 septembre 2020, la Commission avait été saisie par SEM le Ministre d'Etat d'un projet d'Ordonnance Souveraine portant application de la Loi n° 1.491 du 23 juin 2020 relative aux offres de jetons qui a été publiée, au Journal de Monaco, dès le 18 septembre 2020 : Ordonnance Souveraine n° 8.258 portant application de la Loi n° 1.491 relative aux offres de jetons.

A la fin du mois de janvier 2021, la CCIN a été informée d'une modification de l'Ordonnance dès le 29 janvier 2021. Aussi elle a rendu son avis à la lumière des dernières modifications apportées.

La CCIN a relevé que l'appréhension du contexte des offres de jetons requiert l'analyse de plusieurs textes, parmi lesquels : la Loi pour une Principauté Numérique ; la Loi n° 1.491 sur les offres de jetons et son Ordonnance d'application. Or, la multiplicité des interprétations liées aux divers renvois opérés risque, selon elle, d'engendrer une insécurité juridique. La CCIN a d'ailleurs noté une évolution de la terminologie employée entre la Loi n° 1.491 qui se réfère au « *souscripteur* » et l'Ordonnance Souveraine n° 8.258 qui vise l'« *investisseur* ». Elle a également observé que les « *outils techniques mis à disposition par la plateforme* », auxquels renvoie l'Ordonnance Souveraine n° 8.258, doivent encore être précisés par Arrêté Ministériel et que certains éléments de renvoi de la Loi n° 1.491 ne sont pas explicités par l'Ordonnance Souveraine n° 8.258.

Sur le périmètre de labélisation des offres de jetons

La CCIN s'est par ailleurs questionnée sur la cohérence entre la Loi n° 1.491 et son Ordonnance d'application. Les deux premiers articles de la Loi suggèrent en effet, comme cela ressort également du rapport de la Commission du Conseil National pour le Développement du Numérique sur le projet de Loi n° 1.009 concernant les offres de jetons, que le label autorisant la réalisation d'une offre est obligatoire qu'elle soit publique ou privée, qu'elle porte sur des Initial Coin Offerings (ICO) ou des Security Coin Offerings (STO).

[9] Voir supra chapitres dédiés à ces 2 dossiers

Pourtant, le dispositif du projet d'Ordonnance d'application, dont elle a initialement été saisie, prévoyait qu'un label ne soit délivré qu'aux offres d'une valeur atteignant au moins 100.000,00 euros, ce qui était problématique puisque ce même montant minimal servait à distinguer les offres publiques des offres privées de jetons.

Si la Commission a constaté l'abaissement de ce montant à 10.000,00 euros, elle a signalé qu'une telle réévaluation ne permet pas de mettre fin à l'ensemble des problématiques, puisque le dispositif de la Loi n° 1.491 exige que toutes les offres soient labélisées. La Commission s'est notamment interrogée sur la possibilité de créer une offre de jetons en dessous de ce montant et sur l'éventuelle volonté de limiter les offres publiques à des jetons ayant une valeur nominale comprise entre 10.000,00 et 99.000,00 euros. Il lui a pourtant semblé que l'aspiration de l'Ordonnance Souveraine n° 8.258 était de se rapprocher du Règlement AMF (Autorité des Marchés Financiers) du Pays voisin. Aussi, la CCIN a considéré que la référence à la notion d'« *offre privée* » était erronée (cette définition excluant le nombre de participants à l'opération et la qualité des investisseurs) et que l'offre de jetons ne s'adresse non pas « *à des investisseurs qui acquièrent des jetons pour un prix total d'au moins 100.000 euros par investisseur et par offre distincte* », mais à des investisseurs qui s'engagent à acquérir des jetons.

Sur les missions dévolues par le texte à la Direction de l'Expansion Economique

Le périmètre de compétences dévolu à la Direction de l'Expansion Economique (DEE) a, en outre, appelé l'attention de la CCIN. L'article 11 de la Loi n° 1.491 lui confie des pouvoirs de « *contrôle du respect des conditions de l'autorisation délivrée en application du Chapitre I* ». Or, l'article 2 du Chapitre I fait référence à « *une autorisation administrative (...) délivrée par le Ministre d'Etat* » et l'article 5 à « *une plateforme numérique autorisée par le Ministre d'Etat* ».

Les prérogatives de contrôle de la DEE lui sont aussi apparues mal définies, notamment à la lumière de l'article 12 de la Loi n° 1.491 qui permet à ses agents de « *notamment* » se faire communiquer des informations ou consulter les informations accessibles depuis un service de communication au public en ligne. La CCIN s'est demandée si de possibles analyses de sécurité pourraient à cette occasion être confiées à la DEE, d'autant que le document d'informations

accompagnant l'offre (« *White paper* ») contient « *les caractéristiques du dispositif d'enregistrement numérique sur un registre partagé sur lequel les jetons sont émis et les modalités techniques de l'émission des jetons* ».

Sur le Chapitre VI de l'Ordonnance Souveraine n° 8.258 « *Des conditions d'autorisation d'une plateforme numérique* » et la Loi sur la Principauté numérique

La CCIN a notamment relevé que les définitions nécessaires à l'offre de jetons ont été introduites dans la Loi sur la Principauté numérique en lieu et place du projet de Loi relative à la technologie Blockchain. Elle a pourtant constaté que l'article 1er de la Loi n° 1.491 ne fait le lien qu'avec les définitions d'actif numérique, d'actif financier virtuel, qui ne sont d'ailleurs reprises ni dans le dispositif de la Loi ni dans celui de l'Ordonnance n° 8.258, de jeton et de clé privée.

Elle a regretté qu'il faille atteindre l'article 6 de l'Ordonnance Souveraine n° 8.258 pour faire la connexion entre la notion de « *plateforme* » *visée par la Loi n° 1.491 et celle de « dispositif d'enregistrement numérique sur un registre partagé* » inscrite dans la Loi sur la Principauté numérique.

La CCIN, qui n'a pas été consultée sur le projet de Loi relative à la blockchain ou sur l'ajout de ces terminologies au sein de la Loi sur la Principauté numérique, a discerné une confusion sur la nature de service de confiance du dispositif d'enregistrement numérique sur un registre partagé. Elle a ainsi souligné l'absence de définition du dispositif d'enregistrement numérique sur un registre partagé qualifié, alors, qu'à la lecture de définitions présentes dans la Loi sur la Principauté numérique et son article 47, il s'entend comme un service de confiance.

Du reste, elle n'a pas perçu la subtilité d'ériger, en service de confiance, « *la conservation et la gestion de données, documents ou actifs numériques au moyen (...) d'un dispositif d'enregistrement numérique sur un registre partagé* » et le « *dépôt d'actifs numériques sur un dispositif d'enregistrement sur un registre partagé* » semblant relever du même régime de l'article 48 de la Loi sur la Principauté numérique.

Elle a, au demeurant, souligné qu'une telle qualification n'est pas sans conséquence sur la procédure d'autorisation de la plateforme qui est « *un dispositif d'enregistrement numérique sur un registre partagé* » pouvant être qualifié par l'Agence Monégasque de Sécurité Numérique, selon des critères définis par Ordonnance Souveraine. Dans le même temps, selon l'Ordonnance Souveraine n° 8.258, « *les outils techniques mis à disposition par la plateforme numérique sont précisés par Arrêté Ministériel* ». La CCIN s'est ainsi inquiétée d'une possible coexistence d'exigences différentes entre les textes.

Enfin, elle a noté l'exigence d'une ancienneté minimale de la plateforme dans le domaine de l'offre de jetons réalisée susceptible d'acter l'exclusion

de la création d'une plateforme monégasque et aux détours de renvois à des bas de page de l'Ordonnance Souveraine n° 8.258, l'exigence de localisation du dispositif d'enregistrement numérique sur un registre partagé à Monaco qui n'est prévue ni dans le dispositif de la Loi n° 1.491 ni dans celui de l'Ordonnance Souveraine n° 8.258.

Sur les interactions avec les Loi n° 1.338 sur les activités financières et n° 1.362 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption

Elle a de plus discuté la possibilité que la définition des offres de jetons STO et celle d'instrument financier prévue dans la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou

administration d'instruments financiers, puissent intéresser la Commission de Contrôle des Activités Financières (CCAF) dans l'exercice de ses missions. Toutefois, le concours de cette Autorité Administrative Indépendante ne semble pas possible, en l'état des textes qui ne visent que les « *services de l'Administration* » pour porter assistance à la Commission chargée d'instruire les demandes d'autorisation d'offre de jetons. La CCIN s'est de ce fait interrogée sur l'opportunité de compléter la composition de la Commission susvisée au regard de la spécificité, de la technicité et de la complexité des dossiers qui lui seront soumis. Enfin, elle a appelé l'attention du Gouvernement sur la prise en compte de la lutte anti-blanchiment qui, certes mentionnée dans le texte de l'Ordonnance, lui apparaît en retrait par rapport aux évolutions à l'étude dans les pays voisins, ainsi que sur les critères qui serviront à déterminer l'honorabilité, l'expérience et la compétence professionnelle destinés à autoriser ou non une offre de jetons.

Sur le silence des textes ou l'absence de texte sur les technologies mises en œuvre et leurs conséquences sur la protection des informations nominatives

Pour conclure, la Commission a rappelé que rien ne semblait venir expliciter les technologies blockchain utilisées dans les offres de jetons et définies dans la Loi n° 1.383 pour une Principauté numérique avec leur utilisation (clé publique, clé privée, smart contracts), ni encadrer les différences entre ICO et STO. Elle a de ce fait appuyé sur l'existence de réelles conséquences en termes d'informations nominatives exploitées.

LES PROJETS D'ORDONNANCES SOUVERAINES EN LIEN AVEC LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX, LE FINANCEMENT DU TERRORISME ET LA CORRUPTION

La Commission, consultée par le Ministre d'Etat relativement au projet de Loi renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, avait formulé son avis par délibération n° 2020-113 du 1er juillet 2020[10] . Les projets de textes d'application de cette Loi ont ainsi été soumis à la Commission en mars 2021 mais les Ordonnances Souveraines ont été publiées au Journal de Monaco du 29 avril 2021 sans que l'avis de la CCIN n'ait été rendu.

La Commission, bien qu'interpellée par le peu d'intérêt prêté à ses avis par les Services gouvernementaux, et déplorant que les saisines du Gouvernement soient désormais effectuées très fréquemment dans l'urgence, a néanmoins rendu son avis sur les textes concernés :

- l'Ordonnance Souveraine n° 8.634 modifiant l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la Loi n° 1.362 du 3 août 2009, modifiée, relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

- l'Ordonnance Souveraine n° 8.635 portant application de la Loi n° 214 du 27 février 1936 portant révision de la Loi n° 207 du 12 juillet 1935 sur les trusts, modifiée.

Si elle a souhaité rendre néanmoins son avis sur ces 2 textes déjà publiés, c'est essentiellement en considération du fait qu'un projet de Loi avait été déposé afin notamment de corriger des incohérences et des erreurs matérielles dans la Loi n° 1.382, telle que modifiée en fin d'année 2020, erreurs matérielles dont n'est pas exempte l'Ordonnance Souveraine n° 2.318, modifiée au mois d'avril 2021.

[10] Voir rapport d'activité 2020 de la CCIN p 74 et suivantes

Aussi elle a considéré que ce projet de Loi pourrait être l'occasion d'adresser certaines réponses aux remarques de la Commission, et que son avis pourrait utilement être pris en compte pour corriger, préciser ou modifier également certains éléments de l'Ordonnance Souveraine n° 2.318, susvisée.

L'adoption de mesures équivalentes à celles de la Vème Directive et la notion de transparence

La Commission a d'abord rappelé que la Principauté devait adopter dans la matière des mesures équivalentes à la Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la Directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les Directives 2009/138 CE et 2013/36/UE, dites Vème Directive.

Or, elle n'a pu que constater la différence entre l'approche retenue par ce texte européen qui met l'accent sur la transparence des informations sur les Bénéficiaires Effectifs comme moyen de dissuasion à la commission d'infractions, et celle monégasque prévue par l'Ordonnance Souveraine n° 8.634, susvisée.

Le Législateur européen a ainsi pu affirmer que « *l'accès du public aux informations sur les bénéficiaires effectifs permet un contrôle accru des informations par la société civile, notamment la presse ou les organisations de la société civile, et contribue à préserver la confiance dans l'intégrité des transactions commerciales et du système financier* », alors que l'article 63 de l'Ordonnance Souveraine n° 2.318 tel que modifié par l'Ordonnance Souveraine n° 8.634 exige que « *la demande d'information, ses motifs et le lien entre ces derniers et la prévention du blanchiment de capitaux et du financement du terrorisme, sont notifiés par le service du répertoire du commerce et de l'industrie aux personnes morales tenues de communiquer les informations sur leurs bénéficiaires effectifs dans les conditions prévues à l'article 22 et aux bénéficiaires effectifs eux-mêmes* ».

Ainsi, plusieurs conditions sont exigées à Monaco pour accéder au registre des Bénéficiaires Effectifs :

- informer au préalable la personne morale concernée (cette dernière disposant de la possibilité de solliciter une restriction au droit d'accès) ;

- communiquer à cette personne morale des informations portant sur l'identité du demandeur et un « *énoncé des motifs de la demande et son lien avec la lutte contre le contre le blanchiment de capitaux et de financement du terrorisme* ». A cet égard, la Commission s'est inquiétée que cette transmission puisse concerner l'ensemble des informations du formulaire de demande, dont les copies de documents d'identité des personnes sollicitant un accès au registre. Aussi elle a demandé à ce que toute ambiguïté soit levée sur cette faculté qui serait parfaitement disproportionnée et contraire aux dispositions de la Loi n° 1.165 relative à la protection des informations nominatives.

Le Registre des bénéficiaires effectifs

La Commission a constaté que demeuraient, malgré l'adoption des textes d'application de la Loi n° 1.362 modifiée, trop de questions en suspens sur les modalités d'accès au registre des bénéficiaires effectifs.

Concernant les personnes listées à l'article 61-1 de l'Ordonnance Souveraine n° 2.318 modifiée par l'Ordonnance Souveraine n° 8.634, celles-ci doivent-elles remplir un formulaire auprès de la Direction de l'Expansion Economique (DEE), ce qui, a contrario des demandes d'informations prévues aux articles suivants, n'est pas possible ? Le cas échéant, cela conduirait à informer les personnels de la DEE des accès des personnes susvisées agissant dans le cadre d'enquêtes ou de procédures d'instructions.

Concernant les accès logiques au système, quelles sont les modalités encadrant le traitement y relatif mis en œuvre ? Quelle est la durée de conservation des informations de traçabilité générées par les différents acteurs concernés ?

Par ailleurs, en ce qui concerne l'article 62 de l'Ordonnance précitée, il est prévu que les entités assujetties à la Loi n° 1.362 modifiée, qui utilisent ce registre de manière usuelle, puissent se voir communiquer les informations y figurant, cette communication étant « c*onditionnée par la remise au service du répertoire du commerce et de l'industrie d'une déclaration signée par le représentant légal de la personne requérante ou par une personne dûment habilitée en son sein* ».

Sous peine d'irrecevabilité, cette déclaration doit être accompagnée d'une copie d'une pièce d'identité en cours de validité du signataire, ainsi que de toute pièce permettant d'établir que la personne requérante appartient à l'un des organismes ou des personnes visés aux articles premier et 2 de la Loi n° 1.362 du 3 août 2009, modifiée.

A l'heure où le développement de l'usage du numérique tend à se développer en Principauté,

la Commission a considéré que des précisions devraient être apportées sur les modalités pratiques de ces transmissions (papier / support numérique sécurisé/ création d'un compte, ...).

En outre, elle n'a pas souscrit à la nécessité de collecter des informations aussi précises sur les employés et représentants légaux des organismes assujettis et notamment l'adjonction automatique, pour chaque demande opérée par ces derniers, de copies de documents d'identité, qui auront alors vocation à se multiplier de manière disproportionnée, ce qui l'a conduite à estimer que la collecte envisagée était en contradiction avec les principes fondamentaux de protection des données personnelles, d'autant que rien ne vient encadrer les modalités de conservation des formulaires et documents d'identité, ni leur durée de conservation.

Le Registre des comptes de paiement, des comptes bancaires et des coffres-forts

La Commission a constaté que les informations y sont conservées pour 10 ans révolus, après l'enregistrement de la clôture du compte et s'est interrogée sur la pertinence de ce délai.

Elle a considéré par ailleurs que les finalités en lien avec la tenue de ce Registre devraient être expressément rappelées afin de pallier tout risque de détournement de finalité.

En outre, il a été relevé que les modalités d'accès au Registre ne sont pas explicitées, alors que l'article 64-5 de la Loi n° 1.362 prévoit expressément la définition des modalités de fonctionnement et d'accès à ce registre, ainsi que des dispositifs permettant d'assurer la traçabilité de ses consultations, par une Ordonnance Souveraine.

Le Registre des trusts

La Commission a tenu à rappeler que le caractère exact et actuel des données contenues dans le Registre devra être garanti.

De plus il devrait être précisé s'il s'agit d'un accès distant directement ouvert de manière sécurisée sur ledit registre, ou s'il s'agit d'un accès sur place. Dans ce cas, la Commission a constaté que les dispositions ne prévoient pas la délivrance d'un extrait mentionnant les informations concernées, à la différence des « *accès* » effectués par les entités assujetties à la Loi n° 1.362 qui donnent lieu à la communication des informations au demandeur. Sur ce point elle a noté que l'article 13-4 de la Loi n° 214 sur les trusts prévoit la communication dudit extrait par le Ministre d'Etat, là où l'article 7 de l'Ordonnance n° 8.635 mentionne que la communication de ce document est effectuée par le Service en charge du registre des trusts.

Elle a également regretté l'absence d'encadrement de la durée de conservation, par le service émetteur, de la copie de l'extrait.

La vérification de l'identité des personnes physiques ou morales bénéficiaires d'un contrat d'assurance-vie ou de capitalisation

La Commission s'est interrogée sur la distinction qui semble être opérée entre l'identification des bénéficiaires des contrats visés à l'alinéa 1er de l'article 16 de l'Ordonnance Souveraine n° 2.318 modifiée et la/les personnes physiques ou morales bénéficiaires d'un contrat d'assurance-vie, en termes d'identification et de collectes d'informations.

Les modalités de mise en œuvre des mesures de vigilance renforcée applicables aux personnes politiquement exposées

La Commission a noté qu'il est prévu à l'article 24 de l'Ordonnance Souveraine n° 2.318 la détermination par Arrêté Ministériel de la liste des fonctions

publiques importantes qui existent sur le territoire monégasque et des fonctions publiques importantes de chaque Organisation internationale accréditée à Monaco. Il est précisé que cette liste comprend toute fonction importante susceptible d'être confiée à des représentants de pays tiers et d'Instances internationales accrédités par l'Etat.

Aussi elle s'est interrogée sur la possibilité que pourrait avoir le Gouvernement d'étendre la liste prévue au 9ème alinéa de l'article 24 de l'Ordonnance Souveraine. Si la liste ainsi publiée contient une erreur matérielle, comme par exemple des oublis, déliera-t-elle les établissements bancaires de leur obligation de vigilance à l'égard des personnes non inscrites ? La Commission a constaté en outre qu'aucun Arrêté Ministériel d'application n'avait été publié, ce qui l'a conduite à se questionner sur le bien-fondé des mesures de vigilance qui seraient malgré tout mises en œuvre par les entités assujetties à l'égard des personnes politiquement exposées pouvant potentiellement être inscrites sur cette future liste.

Les dispositions particulières aux groupes

La Commission a constaté que les dispositions récemment introduites dans l'Ordonnance Souveraine n° 2.318 font référence à la mise en place, au niveau du groupe, d'une organisation et de procédures internes prévoyant le partage des informations.

Elle a toutefois souligné les difficultés rencontrées du fait de l'imprégnation des dispositions LAB étrangères à Monaco par le biais de ces procédures, ce qui conduit parfois la Commission, pour traiter les dossiers qui lui sont soumis par les entités assujetties, à devoir trancher des problématiques légales relevant des compétences du législateur et, dans leur mise en œuvre, du SICCFIN.

Ainsi, elle a rappelé, une nouvelle fois, qu'elle a à connaître fréquemment de la soumission aux vérifications en matière de LAB des personnels des prestataires des entités assujetties, des candidats

à un emploi au sein de celles-ci, ou de leurs salariés déjà en poste depuis plusieurs années, et ce quelle que soit la nature des fonctions concernées. Ceci l'a amenée à appeler, encore, de ses vœux à une clarification textuelle précise concernant les personnes devant et pouvant être soumises aux vérifications en matière de LAB.

Sa pratique courante des traitements LAB conduit également la Commission à constater que l'introduction de pratiques et de directives de groupes en Principauté peut conduire à clôturer les comptes, ou à refuser l'entrée en relation, à des personnes ayant fait l'objet d'un signalement défavorable par l'une des entités situées à l'étranger, que le motif du signalement soit avéré ou pas, et en lien ou non avec la lutte contre le blanchiment de capitaux, le financement du terrorisme ou la corruption. Aussi elle a tenu à attirer l'attention sur la nécessité pour les personnes concernées de bénéficier d'une procédure locale et autonome.

09

SECTEUR PRIVÉ : FOCUS SUR DES PROBLÉMATIQUES SPÉCIFIQUES

Lors des séances plénières de la Commission ainsi que dans le cadre des réunions avec les responsables de traitement, quelques problématiques spécifiques ont suscité des discussions au cours de l'année 2021.

LA CONFIGURATION DES OUTILS DE MESURE DE L'EXPÉRIENCE UTILISATEUR

Lors de sa réunion du 15 décembre, la Commission s'est prononcée contre la mise en place d'un logiciel de mesure de l'expérience utilisateur qui avait pour objectifs principaux d'anticiper les dysfonctionnements et anomalies des applications et postes de travail, de mesurer l'usage réel des applications pour adapter les licences nécessaires aux besoins avérés et de disposer d'éléments d'alerte sur les failles de sécurité (correctifs non appliqués, antivirus et/ou firewall désactivés) mais conduisait en pratique à un suivi individualisé des utilisateurs, constituant ainsi une surveillance constante et inopportune des salariés.

Si la Commission a relevé que les seules données collectées par le logiciel concernaient uniquement le fonctionnement des applications ou de l'environnement technique (nombre d'interactions, temps de réponse, ...) et la consommation de ressources informatiques de ces applications (puissance de calcul du poste de travail, mémoire, réseau, ...) et que ces données servaient à l'établissement d'indicateurs permettant de déterminer la qualité du fonctionnement de ces applications et de faciliter le diagnostic en cas de dysfonctionnement, elle a toutefois constaté que parmi les données techniques collectées certaines permettaient directement ou indirectement d'identifier l'utilisateur, telles que le login des utilisateurs, l'adresse IP, l'adresse MAC du poste de travail (PC, portable, tablette...), le nom du poste de travail ou encore le numéro de série du PC.

La Commission a par ailleurs remarqué que les données collectées permettaient de calculer des indicateurs agrégés ou par poste de travail et que ceux-ci étaient préalablement définis, et présentés sous forme de tableaux de bord, afin d'analyser par exemple le fonctionnement, ou l'usage des applications et infrastructures du système d'information depuis les postes de travail comme par exemple le nombre d'ouvertures des sessions Windows sur les postes de travail, le temps d'ouverture moyen de ces mêmes sessions sur une période donnée, ou encore certaines informations sur les URLs des sites visités.

L'analyse du dossier a également montré que ce traitement était configuré de sorte à « *surveiller l'utilisateur (employé)* », et qu'à intervalle régulier, l'outil transférait toutes les données collectées vers le serveur dédié à l'analyse de ladite collecte.

Lors de l'inventaire, étaient en effet collectées en temps réel les données des tablettes, téléphones,

ordinateurs, etc., comportant la liste des logiciels installés sur les postes de travail ainsi que les composants logiciels dans le but d'étudier l'utilisation réelle des applications par les utilisateurs afin d'adapter au mieux les achats ou locations de licences.

Cette mesure d'utilisation d'une application était basée sur la notion de « *focus travaillant* » : une application était ainsi considérée comme utilisée « *focus travaillant* » s'il y avait une détection d'évènements système indiquant des actions clavier ou souris et si l'application était en premier plan. En revanche, lorsque l'utilisateur ouvrait une application mais ne bougeait pas la souris ni utilisait son clavier, il était considéré comme « *Focus non Travaillant* ».

La Commission a enfin noté qu'un rapprochement avec d'autres données présentes dans d'autres référentiels permettrait d'identifier les utilisateurs via les postes de travail qu'ils utilisaient et les indicateurs de fonctionnement étaient calculés au niveau de chaque poste de travail permettant de « *rattacher ce poste de travail à un utilisateur* ».

Compte tenu de l'ensemble de ces éléments, elle a émis un refus à la demande d'autorisation qui lui avait été soumise par le responsable de traitement.

LES TRAITEMENTS MIS EN ŒUVRE PAR LES AVOCATS EN MATIÈRE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX

Dans la continuité des déclarations de traitements effectuées par les Avocats de la Principauté, la CCIN a été destinataire, en fin d'année 2021, de formalités liées au traitement de « *Gestion des obligations de vérification aux fins de la prévention du blanchiment de capitaux, du financement du terrorisme et de la corruption* ».

Cette formalité s'inscrit dans la poursuite des échanges survenus, au cours des années 2020 et 2021, entre le Secrétariat Général de la CCIN et le Bâtonnier de l'Ordre des Avocats en exercice.

En effet, en application de l'article 2 de la Loi n° 1.362 du 3 août 2009, modifiée, relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, les dispositions de ce texte sont applicables aux Avocats-Défenseurs, Avocats et Avocats-Stagiaires, lorsqu'ils :

« *- participent, au nom de leur client et pour le compte de celui-ci, à toute transaction financière ou immobilière ou ;*

- assistent leur client dans la préparation ou l'exécution de transactions portant sur :

I) l'achat et la vente de biens immeubles ou d'entreprises commerciales ;

II) la gestion de fonds, de titres ou d'autres actifs appartenant au client ;

III) l'ouverture ou la gestion de comptes bancaires, d'épargne ou de portefeuilles ;

IV) l'organisation des apports nécessaires à la constitution, à la gestion ou à la direction de sociétés ;

V) la constitution, la gestion ou la direction de fiducies/trusts, de sociétés, de fondations ou de structures similaires ».

Le traitement portant sur des soupçons d'activités illicites, des infractions et des mesures de sûreté et pouvant, par ailleurs, comporter des données biométriques nécessaires au contrôle de l'identité des personnes, des demandes d'autorisation ont donc été régularisées, auprès de la CCIN, conformément à l'article 11-1 de la Loi n°1.165 du 23 décembre 1993, modifiée.

Comme pour les formalités liées au traitement métier des Avocats, la CCIN a jusqu'à présent été particulièrement attentive à la sécurisation des communications électroniques en tenant compte de la nature des informations transmises.

10

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.

Participation virtuelle à la 43ème conférence de l'Assemblée mondiale pour la protection de la vie privée

La CCIN a participé du 18 au 21 octobre 2021 de manière virtuelle à la 43ème conférence de l'Assemblée mondiale pour la protection de la vie privée (AMVP) autour du thème « *La protection de la vie privée et des données : une approche axée sur l'être humain* ».

Cette conférence internationale qui a eu lieu pour la première fois en 1979, est constituée d'une séance ouverte à tous les experts dans le domaine de la protection des données puis d'une session fermée réservée aux Autorités de protection des données, ainsi que de plusieurs événements parallèles organisés par les Organisations internationales et les ONG.

L'objectif de la session ouverte de cette conférence était « *de faire en sorte que l'on passe de la protection des données personnelles à la protection de la vie privée des personnes en tant que droit fondamental* », comme l'a déclaré en ouverture l'hôte de la conférence, Blanca Lilia Ibarra Cadena, Présidente-Commissaire de l'Institut national pour la transparence.

La reconnaissance faciale, l'identité numérique les problèmes liés aux collectes d'informations sensibles dans le cadre du Covid-19, l'intelligence artificielle ou encore les transferts internationaux de données ont ainsi été au cœur des discussions des deux premiers jours.

Présidée pour la dernière fois par Elizabeth Denham, Commissaire britannique à l'information, la session fermée a quant à elle réuni près de 90 membres et observateurs venant du monde entier pour discuter des derniers sujets brûlants auxquels les Autorités de protection ont dû faire face ces deux dernières années.

C'est ainsi que dans son discours d'ouverture la présidente sortante a déclaré : « *Nous étions déjà dans une ère axée sur les données, avant même que la pandémie n'amplifie cette accélération de la croissance numérique. Aujourd'hui, l'innovation basée sur les données nous aide à traverser les crises sanitaires et influence toutes les facettes de la société.*

Le travail de notre communauté est au cœur de cela, garantissant que les gens font confiance à cette innovation. Mais nous ne pouvons pas supposer que la vie privée aura toujours une place à la table. Notre contribution aux discussions sur

les principaux problèmes de société dépend de la compréhension que les superviseurs de la protection des données et de la confidentialité apportent un aperçu précieux, un état d'esprit pratique et que nous pouvons répondre rapidement. »

Ces deux jours ont été fructueux puisque plusieurs résolutions ont été discutées et approuvées concernant les droits numériques des enfants, l'accès aux données par les Gouvernements, la coopération internationale en matière d'application de la Loi et les bacs à sable réglementaires.

L'Assemblée a également adopté un plan stratégique pour les deux prochaines années afin de continuer à se concentrer sur la promotion de la confidentialité mondiale, à maximiser l'influence de l'AMVP et à renforcer les capacités des membres.

Les groupes de travail, parmi lesquels le Groupe de Travail sur le Rôle de la Protection des Données Personnelles dans l'Aide Internationale au Développement, l'Aide Internationale Humanitaire et la Gestion de Crise, dont la CCIN assure la Vice-Présidence, ont présenté les activités menées en 2021 et les objectifs pour l'année à venir.

Enfin, des nouveaux membres (le Commissaire à la protection des données, Marché mondial d'Abou Dhabi et le Bureau du Commissaire à l'information du Queensland, Australie) et observateurs ont été admis tandis que le Comité exécutif de l'AMVP a été partiellement renouvelé.

Celui-ci a désormais à sa tête Blanca Lilia Ibarra Cadena, de l'INAI qui a rappelé que l'AMVP « *est vivante et florissante grâce à nos interactions et échanges. Notre partenariat s'approfondit, notre coopération couvrant des questions qui concernent la société dans son ensemble, avec un impact croissant. Les idées exprimées lors de cette conférence nous invitent à repenser et à dessiner de nouveaux horizons sur l'intégration des meilleures pratiques dans le traitement des données personnelle*s ».

Participation virtuelle aux 41ème et 42ème réunions plénières de la Convention 108

Le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatique des données à caractère personnel, plus connu sous le nom de « *Comité de la Convention 108* », a tenu ses 41ème et 42ème réunions plénières par visioconférence, respectivement du 28 au 30 juin et du 17 au 19 novembre 2021.

Plusieurs projets de documents et rapports sur des thèmes aussi cruciaux que l'identité numérique, les clauses contractuelles dans le contexte des flux frontaliers de données ou encore la lutte contre le blanchiment des capitaux et le financement du terrorisme ont été présentés, ce qui a donné lieu à des échanges de vue entre les participants et les experts en charge de ces travaux.

Des Lignes directrices relatives au traitement des données à caractère personnel par et pour les organisations chargées des campagnes politiques ont par ailleurs été finalisées et adoptées afin de fournir des conseils pratiques sur la façon de concilier le droit des électeurs à la vie privée et l'obligation démocratique qui incombe aux organisateurs de campagnes politiques de communiquer avec l'électorat.

Outre des informations relatives à la coopération avec d'autres organes et entités du Conseil de l'Europe, un point a également été fait sur l'état des signatures et ratifications du Protocole d'amendement de la Convention 108, dîte Convention 108+.

Le Comité a également eu l'occasion d'accueillir des personnalités politiques d'importance. C'est ainsi que lors de la session de printemps, la Ministre de la Justice et de la Paix du Costa Rica, Mme Fiorella Salazar Rojas, a fourni des informations sur les évolutions législatives liées à la demande d'adhésion de son pays. De même, en novembre, la Rapporteuse spéciale des Nations Unies sur le droit à la vie privée, Ana Brian Nougrères, a exposé les priorités de son mandat qui a débuté le 1er août 2021 et réitéré son intérêt à collaborer avec le Conseil de l'Europe et le Comité de la Convention 108.

Participation à la 7ème édition des Journées des Réseaux Institutionnels de la Francophonie (RIF)

Un membre du Secrétariat a participé de manière virtuelle à la 7ème édition des Journées des Réseaux Institutionnels de la Francophonie organisées par l'Organisation Internationale de la Francophonie (OIF) les 27 et 28 septembre 2021. Celles-ci ont réuni près de 80 représentants d'institutions membres et experts internationaux autour de 5 thèmes principaux : l'état civil, le renforcement de l'Etat de droit et le respect des droits de l'homme par la prévention et la lutte contre la corruption, les processus démocratiques, le partenariat entre l'OIF et les réseaux institutionnels et enfin la lutte contre la désinformation.

Concernant ce dernier sujet, Mr Chawki Gaddes, Président de l'Instance nationale de protection des données personnelles de Tunisie et Président de l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP), a tenu à mettre en garde contre les réseaux sociaux qui se sont substitués dans nos sociétés connectées aux médias classiques et orientent l'opinion publique à travers notamment la technique du profilage de leurs utilisateurs.

En effet si le ciblage était au début utilisé dans un but commercial, il est aujourd'hui mis en œuvre à des fins politiques afin d'influencer les citoyens comme a pu le démontrer l'affaire Cambridge Analytica.

Afin de lutter contre la désinformation, il propose 4 axes de réponses :

- développer la culture de la protection des données chez les utilisateurs et combattre la phrase « *Moi, je n'ai rien à cacher* » ;
- éradiquer l'addiction aux réseaux sociaux, notamment chez les plus jeunes ;
- créer des réseaux nationaux soumis à la législation nationale ;
- encadrer la recherche des sources des fausses informations qui circulent tout en préservant les données personnelles.

Par ailleurs, citant un proverbe tunisien « *une seule main ne peut pas applaudir* », il a rappelé que la coopération internationale était le seul moyen efficace pour lutter contre les réseaux sociaux et la désinformation.

Participation à la réunion de lancement du Groupe de Travail Monaco de l'AFCDP

Le jeudi 18 mars, les membres du Secrétariat Général ont participé par visioconférence à la réunion de lancement du groupe AFCDP Monaco initialement prévue en avril 2020 dont la vocation première est de permettre à ses membres de partager actualités, questionnements et expériences en matière de conformité au Règlement général sur la protection des données (RGPD) et à la loi interne de protection des données personnelles en Principauté.

L'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) est un des membres fondateurs de la CEDPO (Confederation of European Data Protection Organizations), qui a pour principal objet de promouvoir, au niveau européen, le rôle du délégué à la protection des données personnelles (DPO) en parlant d'une seule voix auprès des Instances européennes, ainsi qu'au niveau national.

Afin d'être au plus proche des réalités du terrain, cette association a souhaité ouvrir un groupe régional dédié aux problématiques de la Principauté.

En tant que Secrétaire Général de la CCIN, Agnès Lepaulmier, s'est réjouie de la constitution de ce groupe et a rappelé que son équipe se tenait à la disposition des responsables de traitement pour les accompagner dans leurs démarches de mise en conformité alors qu'une nouvelle loi en matière de protection des données devrait très prochainement être adoptée.

Après une présentation de l'association par Isabelle Cantero, avocate et administrateur de l'AFCDP, le DPO de la Société des Bains de Mer et du cercle des étrangers de Monaco, a évoqué les difficultés rencontrées au quotidien par les grands groupes internationaux de la Place. Celles-ci incluent notamment la gestion des demandes de suppression des personnes (contraintes légales, pseudonymisation, archivage, traçabilité, anonymisation), le contrôle et la garantie des accès aux données, la gestion des consentements oraux, la qualification des données collectées, la mise à jour des mentions légales, la gestion des cookies prestataires, la mise à jour des processus et procédures internes pour répondre aux nouveaux droits ou encore la création d'un registre des traitements.

Enfin, le Directeur Général d'Actis, s'est attaché à démontrer qu'une mise en conformité réussie

avec le RGDP permettait de renforcer la confiance et l'image d'une société que ce soit sur le plan concurrentiel (hausse de la confiance, différenciation vis-à-vis des concurrents...), organisationnel (amélioration de la structuration de la société, limitation des risques de vol, perte et fuite de données) et juridique (limitation des risques de litiges et de sanctions administratives).

Vice-présidence 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 internationale humanitaire et la gestion de crise

Depuis le début de l'année 2021, la CCIN assure la Vice-Présidence 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 internationale humanitaire et la gestion de crise (« *GT AID* »).

Créé l'année précédente suite à l'adoption d'une résolution de l'Assemblée mondiale pour la protection de la vie privée (« AMVP ») qui regroupe les Autorités de protection des données et de la vie privée, le GT AID s'est réuni trois fois en 2021 et a déjà mené à bien 3 actions principales :

- L'adoption des règles de procédure et de son plan de travail triennal.
- L'établissement d'une cartographie géographique et thématique des acteurs pertinents en matière d'aide au développement et d'aide humanitaire.

Pour ce faire, le groupe de travail a décidé de séparer les principaux acteurs du développement en grandes catégories. D'un côté, les principaux bailleurs qui n'interviennent pas sur le terrain dans la mise en œuvre des programmes, et de l'autre les organisations et opérateurs internationaux qui assurent cette mise en œuvre.

- L'élaboration d'un questionnaire sur les pratiques en matière de protection des données personnelles de ces acteurs pertinents dans la mise en œuvre de leurs programmes et projets.

Ce questionnaire, composé de 16 questions et accompagné d'une lettre qui présente l'AMVP, souligne le fait que le groupe de travail souhaite contribuer à la sensibilisation et à la protection des données et précise qu'il ne s'agit pas d'une initiative réglementaire mais éducative.

Le questionnaire est également accompagné d'une notice explicative contenant les définitions des principaux termes utilisés dans ledit questionnaire et attirant l'attention sur les déclarations du Comité exécutif de l'AMVP.

Pour 2022, les objectifs principaux du groupe de travail sont essentiellement au nombre de quatre :

- Sur la base de la cartographie, collecter les contacts pertinents pour la diffusion du questionnaire ;
- Analyser les réponses au questionnaire et identifier les problématiques urgentes ;
- Si nécessaire, interviewer des acteurs clés tels que le Rapporteur spécial des Nations Unies sur le droit à la vie privée ;
- Maintenir et explorer les synergies possibles avec les autres groupes de travail et les parties prenantes externes.

11

FICHES PRATIQUES

FOCUS SUR LA MESSAGERIE PROFESSIONNELLE AU TRAVAIL

La messagerie professionnelle est aujourd'hui devenue un outil indispensable et bien souvent nécessaire à l'accomplissement, par l'employé, de ses missions de travail. Toutefois, la banalisation d'un tel dispositif de communication électronique n'exonère pas pour autant l'employeur du respect des dispositions relatives à la protection des informations nominatives, et bien qu'il puisse décider de procéder au contrôle ou à la surveillance de l'utilisation de la messagerie mise à disposition de ses salariés, notamment pour des raisons de sécurité, il est tenu également par l'obligation de respecter la vie privée de ces derniers.

En Principauté, en effet, conformément à l'article 22 de la Constitution, « *Toute personne a droit au respect de sa vie privée et familiale et au secret de sa correspondance* ».

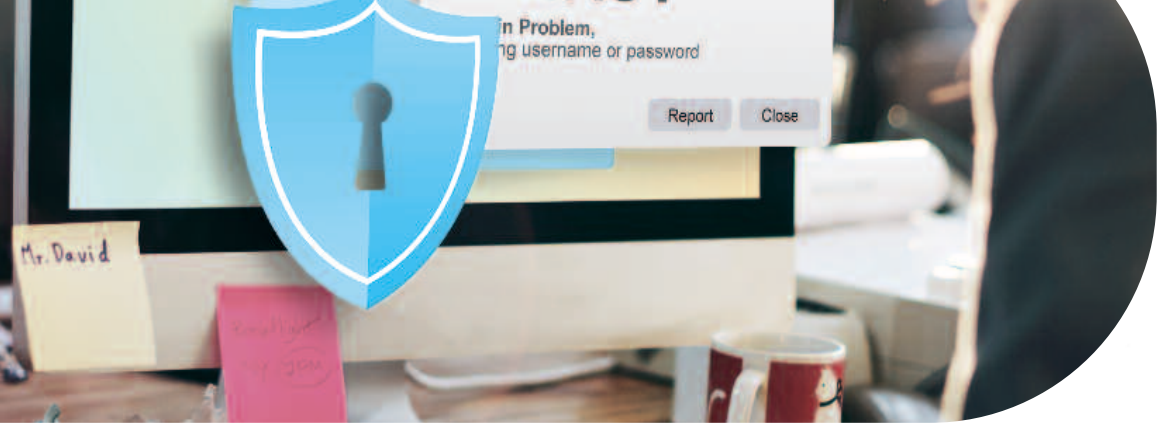
De même, dans un arrêt *Niemietz c. Allemagne* en date du 16 décembre 1992, la Cour Européenne des Droits de l'Homme (CEDH) a consacré le droit au respect de la vie privée sur le lieu de travail en se fondant sur l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, aux termes duquel « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».

Quelques années plus tard, cette même Cour a précisé les conditions dans lesquelles l'employeur peut consulter les communications numériques de son salarié dans son arrêt *Bărbulescu c.* Roumanie en date de 2017.

En l'espèce, un salarié qui avait communiqué avec sa famille à partir de son poste de travail, sur un compte de messagerie destiné à un usage professionnel, avait été licencié, au motif qu'il n'avait pas respecté le règlement intérieur qui interdisait l'utilisation des ressources de l'entreprise à des fins personnelles.

La Cour a toutefois estimé que ce licenciement était contraire au droit à la protection de la vie privée, consacré à l'article 8 de la Convention européenne des droits de l'homme puisque si l'employeur est en droit de surveiller les communications électroniques de son salarié, l'étendue de la surveillance et le degré d'intrusion dans la vie privée du salarié ne doivent pas être disproportionnés par rapport au but recherché. Par ailleurs, il incombe aux juges de vérifier que l'accès au contenu des communications n'a été mis en place que parce qu'il n'existait pas de mesures moins intrusives, et de s'assurer que les conséquences de la surveillance pour le salarié ne sont pas disproportionnées par rapport au but recherché.

Pour tout responsable de traitement, entrent ainsi en conflit deux intérêts apparemment contradictoires, mais néanmoins conciliables, à savoir d'un côté le droit au respect de la vie privée et au secret des correspondance des employés et d'un autre le respect des intérêts légitimes de l'employeur, entre lesquels il convient de trouver un juste équilibre.



Cette fiche pratique a donc vocation à résumer les droits et obligations des employeurs vis-à-vis de leurs employés s'agissant de l'utilisation de la messagerie électronique professionnelle.

➢ *Principe de la protection des correspondances privées sur le lieu de travail*

Pour la Commission, le respect du secret des correspondances privées est un principe intangible. Ainsi, l'employeur ne peut accéder aux contenus des messages privés de ses employés envoyés ou reçus à partir de la messagerie professionnelle, sans que ledit employé soit présent, et en soit expressément d'accord.

Toutefois, pour que les messages soient considérés comme personnels, il convient pour les employés de les identifier comme tels, par exemple :

- en précisant dans l'objet du message des mots clés comme « privé », « ***[PRV]*** » ou encore « ***personnel*** » ;
- en incluant dans l'objet du message une mention laissant manifestement supposer que ledit message est privé, telle que « *vacances au Japon* » ;
- en stockant les messages dans un répertoire intitulé « personnel » ou « *privé* ».

La Commission considère donc comme excessive la pratique consistant pour l'employeur à recevoir tous les messages envoyés ou reçus par ses employés puisque cette pratique ne permet pas de distinguer entre les messages professionnels et personnels desdits employés.

Par ailleurs, seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés lorsque ces derniers n'ont pas autorisé l'employeur à lire leurs messages privés, et cela même si l'employeur a des motifs légitimes de suspecter des actes de concurrence déloyale ou toute autre atteinte portée à ses intérêts ou à la Loi. Cela peut notamment prendre la forme d'une Ordonnance judiciaire mandatant un huissier de justice aux fins d'accéder, voire d'enregistrer les messages privés litigieux.

➢ *Fonctionnalités autorisées*

La Commission estime que tout traitement automatisé de messagerie professionnelle peut notamment avoir les fonctionnalités suivantes :

- l'échange de messages électroniques en interne ou avec l'extérieur ;
- l'historisation des messages électroniques entrants et sortants ;
- la gestion des contacts de la messagerie électronique ;
- la gestion des dossiers de la messagerie et des messages archivés ;
- l'établissement et lecture de fichiers journaux ;
- la gestion des habilitations d'accès à la messagerie ;
- la gestion de l'agenda ;
- l'établissement de preuves en cas de litige avec un client/employé (en cas de contestation d'un ordre, etc..).

Par ailleurs, lorsqu'une surveillance est mise en œuvre sur le lieu de travail, la messagerie professionnelle peut également avoir également pour fonctionnalité(s) :

- la mise en place d'une procédure de contrôle gradué ;
- le contrôle au moyen d'un logiciel d'analyse des messages électroniques entrants ou sortants.

Quid de la notion de surveillance ou de contrôle

Un employeur peut décider de procéder au contrôle ou à la surveillance de l'utilisation de la messagerie professionnelle mise à la disposition de ses employés.

A cet égard, la Commission indique que cette notion de contrôle ou de surveillance de la messagerie électronique se conçoit comme « *toute activité qui, opérée au moyen d'un logiciel d'analyse du contenu des messages électroniques entrants et/ou sortants, consiste en l'observation, la collecte ou l'enregistrement, de manière non occasionnelle, des données à caractère personnel d'une ou de plusieurs personnes, relatives à des mouvements, des communications ou à l'utilisation de la messagerie électronique* ».

➢ *Dispositions à prendre en cas d'absence de l'employé*

Afin d'assurer la continuité des affaires de l'entreprise pendant l'absence d'un salarié (congés, maladie…), la Commission estime que l'employeur pourra avoir accès aux messages professionnels dudit salarié, en utilisant une des méthodes suivantes :

- mise en place d'une réponse automatique d'absence du bureau à l'expéditeur avec indication des personnes à contacter en cas d'urgence ;
- désignation d'un suppléant qui dispose d'un droit d'accès personnalisé à la messagerie de son collègue ;
- transfert à un suppléant de tous les messages entrants.

Dans les deux derniers cas, le salarié devra toutefois être informé de l'identité de son suppléant et ce suppléant ne devra pas lire les messages identifiés comme privés ou personnels.

➢ *Modalités d'information des utilisateurs*

Tout employeur doit impérativement responsabiliser les utilisateurs à la protection de leurs informations nominatives. Dans un souci de transparence envers les utilisateurs, ainsi que de loyauté dans la collecte et le traitement des informations nominatives, la Commission recommande donc à l'employeur de mettre en place une charte d'usage des outils de communication électronique, venant préciser, notamment :

- les modalités d'identification des messages privés ;
- la procédure d'accès à la messagerie par des personnes habilitées, en cas d'absence temporaire ou définitive de l'utilisateur, et ce afin d'assurer la continuité des activités.

➢ *Modalités d'information des tiers destinataires*

La Commission recommande l'insertion d'une mention d'information au bas de tout message électronique sortant, afin d'informer les tiers destinataires de la finalité du traitement, ainsi que de leurs droits.

Exemple de message

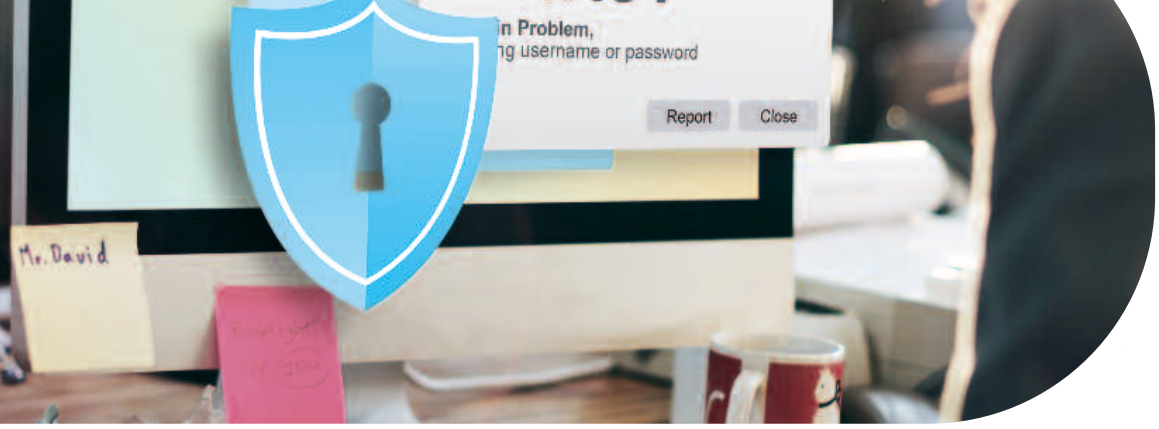
Vos informations nominatives sont exploitées par [Nom de l'employeur] dans le cadre du traitement ayant pour finalité "[Finalité du traitement] ". Conformément à la Loi n° 1.165 du 23 décembre 1993, vous disposez d'un droit d'accès, de rectification et de suppression en écrivant [adresse de l'employeur].

➢ *Données collectées*

La Commission considère que les catégories suivantes de données peuvent être collectées et traitées :

➢ Données communes à l'ensemble des messageries :

- identité : nom, prénom, identifiant ;
- messages : date, heure, information expéditeurs/destinataires, contenu, objet ;
- gestion des contacts : nom, prénom, raison sociale, (…) ;



- données d'identification électronique : adresse de messagerie électronique ;
- journalisation des accès : logs de connexion des personnels habilités à avoir accès au traitement;
- fichiers journaux : date et heure du message, nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeurs de messages, (...) ;
- habilitations : identité des personnes habilitées à avoir accès à la messagerie, type de droits conférés ;

➢ Données particulières aux messageries mises en œuvre à des fins de surveillance ou de contrôle :

- gestion des alertes : réception des alertes automatiques en fonction des niveaux hiérarchiques concernés.

➢ *Durées de conservation des données*

La Commission rappelle que conformément à l'article 10-1 de la Loi n° 1.165, modifiée, les informations nominatives ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont exploitées.

Ainsi, au regard des fonctionnalités de la messagerie, la Commission demande au responsable de traitement de prévoir les durées de conservation de données suivantes :

➢ s'agissant de l'administration de la messagerie électronique (identité, gestion des contacts, données d'identification électronique) : 3 mois **maximum** après le départ définitif de l'utilisateur.

A cet égard, la Commission rappelle que lors du départ définitif de l'utilisateur, sa boite email nominative doit être immédiatement « ***bloquée*** » c'est à dire qu'elle ne doit plus pouvoir recevoir d'emails, ni en envoyer, à l'exception d'un message automatique qui sera adressé à chaque personne ayant envoyé un email à l'adresse concernée.

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

A l'échéance de cette période de trois mois maximum, l'adresse email nominative de l'ancien salarié sera désactivée (supprimée).

L'employeur doit avertir l'employé de la date de fermeture de son compte et lui permettre de récupérer les emails privés susceptibles de se trouver dans sa boite email nominative professionnelle.

- s'agissant du contenu des messages émis et reçus : entre 2 et 3 ans maximum dans la boite active de l'utilisateur puis ensuite, si besoin, mettre en place une **politique d'archivage.**

La Commission reconnait en effet que les messages électroniques des collaborateurs peuvent être conservés durant plusieurs années notamment en ce qui concerne les établissements bancaires et assimilés à des fins de traçabilité des opérations financières, ou en cas de soupçons d'activités illicites.

Les messages récents peuvent être stockés dans la messagerie interne du collaborateur pendant une période n'excédant pas 3 ans maximum (archives courantes) puis être automatiquement effacés de sa messagerie, afin d'être conservés dans un serveur distinct jusqu'à l'expiration du délai nécessaire (archives intermédiaires) avec des accès restreints aux seules personnes ayant un intérêt à en connaître en raison de leurs fonctions (par exemple, le service du contentieux).

- s'agissant de la journalisation des accès et des fichiers journaux : de 3 mois à 1 an maximum, en fonction de l'activité exercée.

- s'agissant des alertes : la Commission demande que les données relatives à un évènement ne mettant pas en lumière un incident (faux positifs par exemple) soient immédiatement supprimées après analyse.

En cas d'incident avéré les données doivent être conservées le temps nécessaire à la réalisation de l'enquête associée, conformément à la législation applicable.

- s'agissant des habilitations : le temps de l'affectation.

En tout état de cause, la Commission recommande, lorsque cela est possible, d'adopter une durée de conservation moindre, dès lors que les

données traitées ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été initialement collectées.

Enfin, la Commission rappelle que dans le cadre de l'ouverture d'une procédure contentieuse, toute information nécessaire issue du traitement pourra être conservée jusqu'à la fin de ladite procédure.

➢ Mesures de sécurité à mettre en place

La Commission rappelle que les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du traitement.

Les mots de passe doivent être forts et régulièrement renouvelés.

Les accès à distance à la messagerie doivent être sécurisés.

L'employeur doit régulièrement sensibiliser les utilisateurs à la sécurité de leur messagerie (par exemple : ne jamais ouvrir les pièces jointes provenant d'un expéditeur inconnu, ne pas cliquer sur des hyperliens dans les emails, ne pas envoyer de données sensibles ou importantes par email non sécurisé).

COMMENT RÉCUPÉRER UN COMPTE FACEBOOK OU INSTAGRAM PIRATÉ ?

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

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

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

COMPTE FACEBOOK PIRATÉ

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

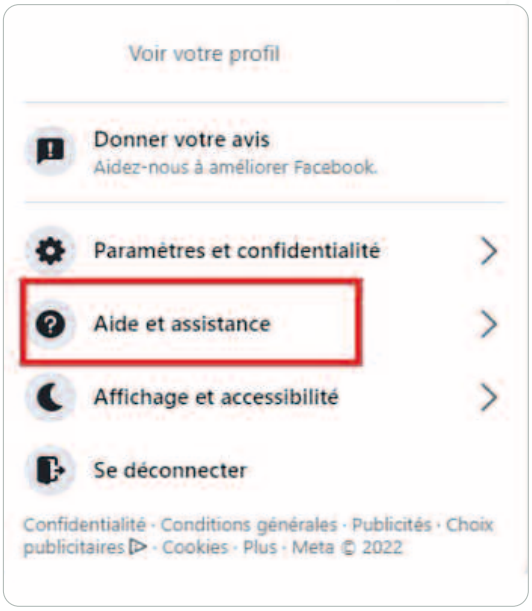
Cas de figure n° 1 : Vous pouvez toujours vous connecter à votre compte Facebook

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

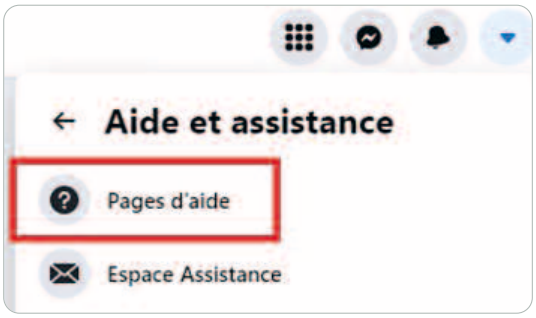
Cette procédure est la suivante :

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

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

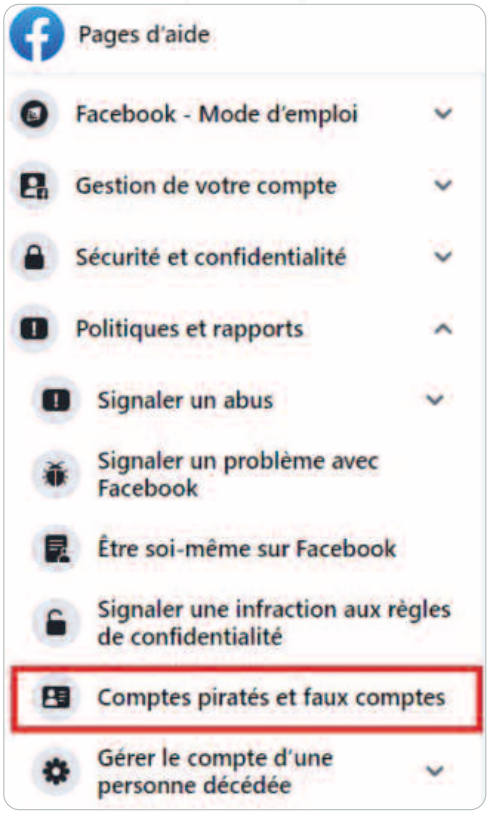


- Cliquez ensuite sur Pages d'aide.

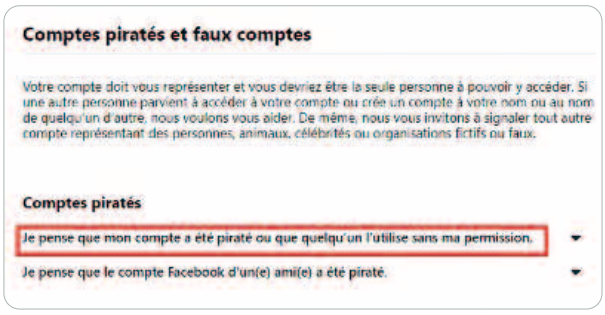


- Dans le menu déroulant, sélectionnez **Politiques et rapports**.

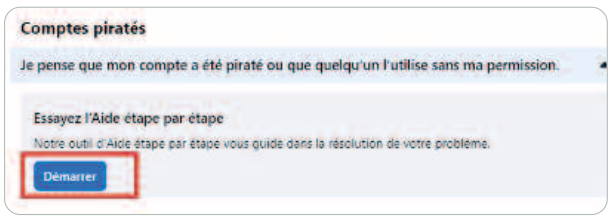
- Un nouveau menu déroulant apparaît. Cliquez sur **Comptes piratés et faux comptes**.



- Une nouvelle page apparaît. Sélectionnez : **Je pense que mon compte a été piraté ou que quelqu'un l'utilise sans ma permission.**



- Cliquez sur **Démarrer.**



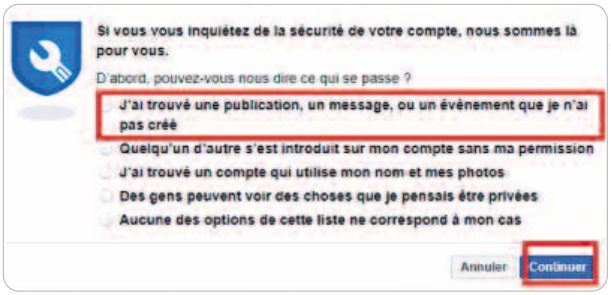
A partir de là, Facebook va vous accompagner étape par étape pour vous permettre de réinitialiser votre mot de passe.

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

Si votre adresse email ou votre mot de passe a été modifié, il convient de lancer une **procédure de récupération de compte.**

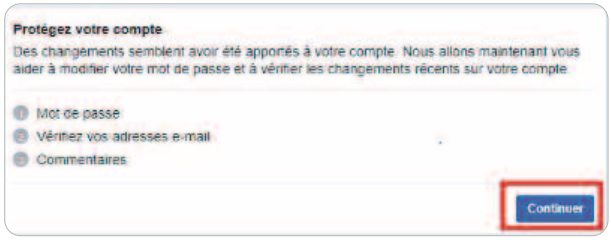
Cette procédure est la suivante :

- Avec votre navigateur Web, allez sur la page spéciale Facebook Hacked (https://www.facebook.com/hacked).
- Une page apparaît. Cochez la 1ère case **J'ai trouvé une publication, un message, ou un évènement que je n'ai pas créé puis cliquez sur Continuer.**



- Une nouvelle page apparaît. Cliquez sur Démarrer.

- Un message vous informe des différentes étapes de la procédure. Cliquez sur **Continuer**.



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

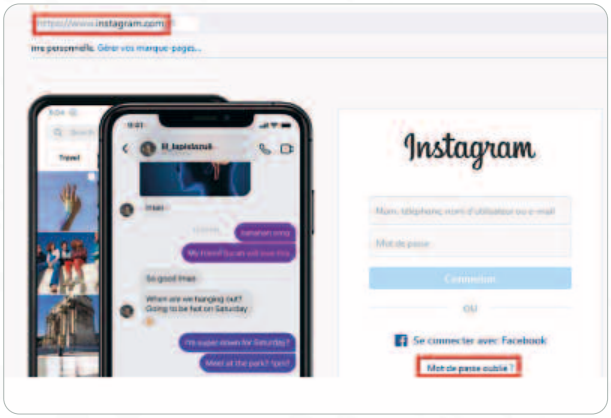
COMPTE INSTAGRAM PIRATÉ

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

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

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

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



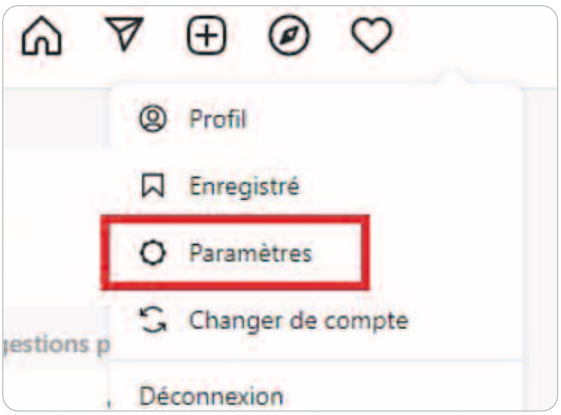
- Saisissez l'adresse email, le numéro de téléphone ou le nom d'utilisateur associé à votre compte, puis appuyez sur Envoyer un lien de connexion..

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

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

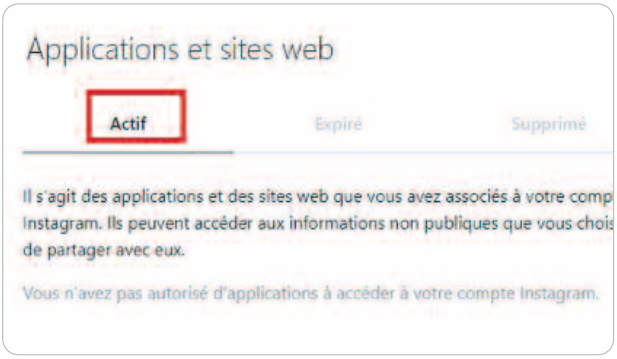
Une fois votre compte récupéré, il est important de le sécuriser en annulant l'accès de certaines applications tierces audit compte.
Pour vérifier les accès accordés, il suffit de suivre la procédure suivante :

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



- Une page apparaît. Dans la colonne de droite, cliquez sur **Apps et sites web.**

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



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

- La première étape est de consulter votre boite e-mail (celle que vous avez utilisé pour créer votre compte Instagram) pour voir si vous avez reçu un message d'Instagram.

- Si vous avez reçu un e-mail d'Instagram vous informant que votre adresse e-mail a été modifiée, vous pouvez annuler cette action à l'aide de l'option **annuler ce changement**.

- Plusieurs options de récupération pourront vous être proposées en fonction de votre compte et de votre sécurité :

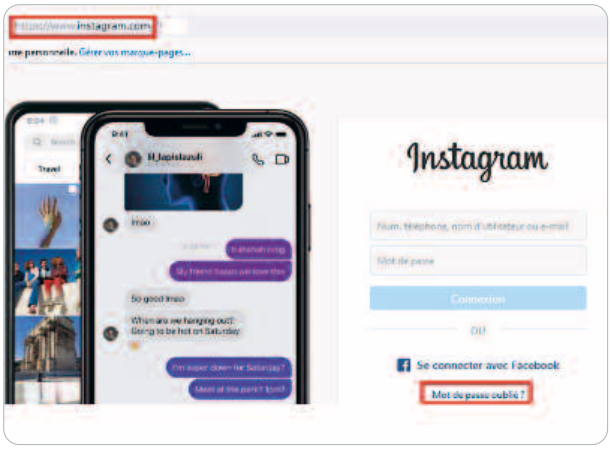
➢ Envoyer une photo de vous tenant une copie manuscrite du code que Instagram vous a fourni.

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

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

- Si d'autres informations ont également été modifiées (par exemple, votre mot de passe) et que vous ne pouvez pas annuler le changement de votre adresse e-mail, signalez sur votre téléphone portable le compte à Instagram.

- Sur la page d'accueil de connexion, cliquez sur **Mot de passe oublié** (iPhone) ou **Se connecter** (Android).



- Sur iOS (iPhone), il faudra ensuite cliquer sur **Envoyer un lien de connexion**, puis **Besoin d'aide supplémentaire ?** et enfin suivre les instructions à l'écran.

- Sur Android, il faudra ensuite cliquer sur **Obtenir de l'aide pour se connecter**, saisir votre nom d'utilisateur, adresse e-mail ou numéro de téléphone, appuyer sur **Suivant** puis sur **Besoin d'aide supplémentaire ?** et enfin suivre les instructions à l'écran.

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

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

- ***Choisissez un mot de passe fort***. Utilisez une combinaison d'au moins six chiffres, lettres et signes de ponctuation (tels que ! et &). Ce mot de passe doit être différent des autres mots de passe que vous utilisez ailleurs sur Internet.

- **Changez de mot de passe régulièrement**, en particulier si vous recevez un message d'Instagram vous invitant à le faire.

- **Ne communiquez jamais votre mot de passe** à une personne que vous ne connaissez pas ou en laquelle vous n'avez pas confiance.

- **Activez l'authentification à deux facteurs**

- **Assurez-vous que votre boîte mail est sécurisée**. Toute personne qui peut lire votre e-mail peut probablement également accéder à votre compte Instagram. Changez le mot de passe de vos comptes de messagerie électronique et assurez-vous d'utiliser un mot de passe différent pour chacun d'eux.

- **Déconnectez-vous d'Instagram lorsque vous partagez un ordinateur** ou un téléphone avec d'autres personnes. Sur un ordinateur public, ne cochez jamais la case « *Mémoriser* », étant donné que cette option vous permet de rester connecté(e) même lorsque vous avez fermé la fenêtre du navigateur.

Si toutes ces démarches devaient toutefois rester infructueuses, vous pouvez contacter la CCIN.

RAPPORT D'ACTIVITÉ

PUBLIÉ EN APPLICATION DE L'ARTICLE 2-14 DE LA LOI N° 1.165

RELATIVE À LA PROTECTION DES INFORMATIONS NOMINATIVES

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

7, rue Suffren Reymond
Immeuble Le Suffren - Bloc B
98000 Monaco
Tél. : +377 97 70 22 44
ccin@ccin.mc - www.ccin.mc