PROTÉGER | INFORMER | PRÉVENIR

CCIN

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

RAPPORT D'ACTIVITÉ 2019

11ème rapport public

www.ccin.mc

Le message du président

2019 a constitué l'année de fin des mandats des Commissaires nommés au mois de juin 2014. Conformément à la feuille de route qu'elle avait définie au moment de son installation il y a cinq ans, la Commission et ses Services sont parvenus à renouer le dialogue avec l'ensemble des entités publiques et privées de la Principauté.

Dans sa nouvelle composition largement reconduite en 2019, la Commission poursuivra ses échanges toujours constructifs, mais jamais complaisants, afin de continuer à accompagner tous les responsables de traitements pour leur permettre de relever les défis qui s'ouvrent à eux, en plaçant la défense des droits et des libertés au cœur de ses décisions.

A cet égard, des réunions ont eu lieu au cours de l'année écoulée avec le Département de l'Intérieur et la Direction de la Sûreté Publique afin d'évoquer les bases textuelles qui seraient nécessaires et suffisantes pour permettre l'exploitation par les Services de Police de dispositifs potentiellement très intrusifs pour les personnes concernées. A l'issue de ces discussions la Commission a souligné que seul un texte législatif explicite et précis serait de nature à permettre l'utilisation des dispositifs envisagés, ce dont le Gouvernement a pris acte publiquement en fin d'année. Dans ce cadre la Commission devrait donc être prochainement saisie d'un projet de Loi sur lequel elle portera bien évidemment une attention toute particulière.

Par ailleurs, la Commission n'a pas manqué de relever l'ambitieux programme de développement du numérique souhaité par le Gouvernement Princier, qui s'est traduit notamment par l'ouverture de nouveaux téléservices, la mise à disposition d'applicatifs ouverts aux usagers, et surtout par l'adoption en fin d'année 2019 de deux Lois relatives à la Principauté Numérique et à l'Identité Numérique. Aussi, la Commission et moi-même avons à cœur d'accompagner ce développement numérique et économique de la Principauté dans le rôle qui est le nôtre, afin que cette nouvelle orientation ne se fasse pas en portant atteinte aux droits et aux libertés des usagers de la Principauté.

La Commission a pu rappeler ces grands principes lors des avis qu'elle a rendus sur les deux projets de Lois relatifs aux textes susvisés. C'est également le message qu'elle a pu adresser au Délégué Interministériel chargé de la Transition Numérique lors de sa visite à notre Commission courant 2019, soulignant que le numérique doit être utilisé au bénéfice des personnes concernées, et non à leur détriment.

Enfin, les travaux relatifs à la refonte de la législation en matière de protection des données personnelles se sont poursuivis tout au long de l'année dans le cadre de réunions régulières entre les Services de l'Etat et de la CCIN, au travers du Groupe de travail ad hoc constitué début 2018. Cette association précoce a permis à la Commission de faire valoir ses souhaits et ses points d'attention spécifiques au regard des standards européens régissant la matière. J'espère vivement qu'ils seront pris en compte dans le texte définitif dont l'entrée en vigueur, très attendue par les acteurs de la Place, va également modifier très profondément les missions de notre Commission.

Je sais que la future Autorité de protection pourra compter sur la parfaite implication de ses Services dont la réorganisation a d'ores et déjà été initiée afin de préparer ces évolutions structurelles.

Je sais également qu'elle aura à cœur d'accompagner au mieux les responsables de traitements face au changement de paradigme porté par la future législation.

Guy MAGNAN

RAPPORT D'ACTIVITÉ

2019

11ème rapport public

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

LA COMPOSITION DE LA COMMISSION

Les articles 4 et 5 de la Loi n° 1.165 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.

De gauche à droite : Agnès Lepaulmier Stefanelli, Secrétaire Général ; Jean-François Cullieyrier, Commissaire ; Jean-Yves Peglion, Commissaire ; Rainier Boisson, Vice-Président ; Guy Magnan, Président ; Florestan Bellinzona, Commissaire ; Philippe Blanchi, Commissaire.

Guy **MAGNAN** - Président

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

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

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

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

Au cours de son mandat 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 assume depuis le mois d'octobre 2018 la Présidence du Conseil du Patrimoine.

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, et desormais de Vice-Président du Tribunal de Première Instance.

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. Il préside également les audiences de flagrant délit.

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.

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.

Jean-Yves **PEGLION** - Commissaire

Titulaire d'un Diplôme d'Etudes Commerciales Supérieures Jean-Yves Peglion débute sa carrière au sein du Service du Personnel du Centre Hospitalier Princesse Grace avant d'intégrer l'Office Monégasque des Téléphones puis la Direction du Budget et Trésor en qualité de Chef de Section.

En 1995 il retourne à l'Office Monégasque des Téléphones au sein de la Direction Administrative et Financière puis il accède aux fonctions de Vérificateur Principal des Finances au Contrôle Général des Dépenses avant d'intégrer la Mairie dont il sera le Secrétaire Général jusqu'en avril 2013, date à laquelle il prend sa retraite.

Nommé Membre de la CCIN en juin 2014 sur proposition du Conseil Communal, sa parfaite connaissance de l'Administration et de la Commune permet utilement à la Commission d'appréhender le traitement des données personnelles par les entités publiques en ayant à l'esprit le nécessaire équilibre entre préservation de la vie privée et fonctionnement des Services Publics.

Au mois de juin 2019 son Mandat a été renouvelé pour une durée de cinq ans, également sur présentation du Conseil Communal.

1

LES MISSIONS ET LE FONCTIONNEMENT DE LA COMMISSION

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

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.

La Convention 108 du Conseil de l'Europe a pour vocation de faire respecter les droits fondamentaux de toute personne, notamment le droit à la vie privée, à l'égard de traitements automatisés de données à caractère personnel la concernant.

Le Protocole additionnel à la Convention 108 relatif aux Autorités de contrôle et aux flux transfrontières de données prévoit, quant à lui, l'instauration par les Etats signataires d'une Autorité de contrôle indépendante chargée de veiller au respect de ses dispositions.

La Convention 108 et son Protocole additionnel ont été ratifiés par la Principauté en décembre 2008. Concomitamment la Loi n° 1.353 du 4 décembre 2008 a érigé la Commission de Contrôle des Informations Nominatives en Autorité Administrative Indépendante soustraite, dans l'exercice de ses compétences, à tout pouvoir de tutelle ou hiérarchique de la part du pouvoir exécutif.

La Loi n° 1.165 du 23 décembre 1993, modifiée par la Loi n° 1.353 du 4 décembre 2008, a consacré de nouvelles dispositions visant notamment à modifier la composition de la Commission et à étendre ses missions et ses pouvoirs.

Afin d'élargir la représentativité des Membres de la Commission et d'asseoir son indépendance, les Institutions chargées de proposer un Membre ont été étendues. Ainsi les Membres qui étaient précédemment proposés par le Ministre d'Etat, le Conseil National et le Conseil d'Etat, le sont désormais également par le Conseil Communal, le Conseil Economique et Social et le Directeur des Services Judicaires qui doit, quant à lui, proposer un Membre ayant qualité de Magistrat du siège.

La durée du mandat des Membres a été portée de trois ans renouvelable sans restriction, à cinq ans renouvelable une fois. De plus le Président est désormais élu par ses pairs et non plus nommé par Ordonnance Souveraine.

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

La Commission a une mission d'information : l'article 2-11° de la Loi précitée dispose en effet qu'elle informe les personnes concernées des droits et obligations issus de ladite Loi, notamment par la communication sur demande à toute personne, ou par la publication, si la Commission l'estime utile à l'information du public de ses délibérations, avis ou recommandations de portée générale, sauf lorsqu'une telle communication ou publication serait de nature à porter atteinte à la sécurité publique ou au respect dû à la vie privée et familiale.

Ainsi, depuis la Loi n° 1.353 entrée en vigueur le 1er avril 2009, les décisions rendues par la Commission ne sont plus confidentielles et sont devenues communicables.

Conformément à l'article 2-14° de la Loi n° 1.165 la Commission a également pour mission d'établir :

- des rapports publics sur l'application de ladite Loi et des textes pris pour son application ;
- un rapport annuel d'activité remis au Ministre d' Etat et au Président du Conseil National, qui est publié.

Ces missions vont dans le sens d'une plus grande transparence dans un domaine sensible au regard des libertés individuelles.

UNE MISSION DE PROPOSITION ET DE CONSULTATION

La Commission a également des missions de proposition et de consultation. A cet effet elle est consultée, conformément à l'article 2-14° de la Loi n° 1.165, par le Ministre d'Etat lors de l'élaboration de textes susceptibles d'avoir une incidence sur 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.

La CCIN peut également :

- formuler toute recommandation entrant dans le cadre des missions qui lui sont conférées par la Loi, afin d'orienter les responsables de traitements en portant à leur connaissance des principes auxquels devraient répondre leurs traitements automatisés ;
- proposer aux Autorités compétentes des dispositions afin de fixer, soit des mesures générales propres à assurer le contrôle et la sécurité du traitement, soit des mesures spéciales ou circonstancielles, y compris, à titre exceptionnel, la destruction des supports d'informations ;

- proposer ou donner un avis sur l'édiction de normes fixant les caractéristiques auxquelles doivent répondre les traitements ne comportant manifestement pas d'atteinte aux libertés et droits fondamentaux. Ces traitements peuvent faire l'objet d'une déclaration simplifiée de conformité, ou être exonérés de toute obligation de déclaration, dans les conditions prévues par Arrêté Ministériel.

UNE MISSION DE CONTRÔLE *A PRIORI*

La première phase de ce contrôle relève de l'analyse du caractère complet du dossier de formalité. Elle est effectuée par le Secrétariat Général, conformément à l'Ordonnance d'application de la Loi n° 1.165.

L'analyse porte sur la vérification des éléments limitativement énumérés à l'article 8 de la Loi n° 1.165.

Dans le cadre de la seconde phase de contrôle a priori, la Commission analysera l'ensemble du traitement soumis à demande d'avis ou d'autorisation et appréciera si les principes relatifs à la qualité des informations, aux conditions de licéité des traitements et au respect des droits des personnes sont garantis ; elle vérifiera également si les exigences de sécurité et de confidentialité des traitements sont remplies.

Même si la dichotomie entre traitements du secteur public et assimilé (organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires de Service Public) et traitements du secteur privé persiste avec la Loi n° 1.165, les uns étant soumis à l'obtention d'un avis favorable de la Commission et les autres à une obligation déclarative, les acteurs du secteur public et assimilé comme ceux du secteur privé sont désormais soumis à un régime d'avis pour les traitements qui ont pour objet de procéder à des « *recherches dans le domaine de la santé* », tel que prévu à l'article 7-1 de ladite Loi, afin de mettre en place une protection spécifique dans un domaine sensible.

La Commission a par ailleurs été investie par la Loi n° 1.165, d'un pouvoir d'autorisation, ce régime est visé :

- à l'article 11-1 pour la mise en œuvre par les personnes physiques ou morales de droit privé :

- de traitements portant sur des soupçons d'activités illicites, des infractions et des mesures de sûreté ;
- de traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes ;
- de traitements exploités à des fins de surveillance ;

- à l'article 20-1 pour les transferts d'informations nominatives vers des Pays ou organismes n'assurant pas un niveau de protection adéquat.

UNE MISSION DE CONTRÔLE *A POSTERIORI* : LES INVESTIGATIONS

Deux procédures distinctes

L'investigation à l'initiative de la Commission

L'article 18-1 de la Loi n° 1.165, introduit par la Loi n° 1.420, définit le cadre des investigations « *préventives* », que la CCIN effectue 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.

Toutefois, en cas d'urgence ou de risque imminent de destruction ou de disparition de pièces ou de documents, les investigateurs pourront accéder aux locaux sans autorisation préalable du Juge, lequel pourra cependant être saisi par les personnes auxquelles les opérations de contrôle feraient grief aux fins de déclarer la nullité desdites opérations, par exemple en cas d'invocation manifestement injustifiée de l'urgence.

L'investigation suite à une plainte

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.

Un socle commun

Le nouvel article 18 de la Loi n° 1.165 définit le cadre commun à ces deux types de contrôles sur place et introduit un certain nombre de nouveautés par rapport aux précédentes dispositions.

Une plage horaire élargie

Comme auparavant, les investigations pourront se dérouler entre 6h00 et 21h00, mais également en dehors de ces heures lorsque l'accès au public est autorisé ou qu'une activité est en cours.

L'opposabilité du secret professionnel

L'opposabilité du secret professionnel a également été introduite ; cependant l'exposé des motifs de la Loi n° 1.420 vient préciser que les personnes opposant à la CCIN le secret professionnel devront préciser les dispositions législatives ou réglementaires auxquelles elles se réfèrent et les informations qu'elles estiment couvertes par ces dispositions, l'invocation injustifiée du secret professionnel pouvant constituer un délit d'entrave.

Les missions lors du contrôle

Lors des opérations de contrôle les investigateurs peuvent procéder à toutes vérifications nécessaires, consulter tout traitement, demander communication, quel qu'en soit le support, ou prendre copie, par tous moyens, de tout document professionnel et recueillir, auprès de toute personne compétente, les renseignements utiles à la mission. Ils peuvent accéder aux programmes informatiques et aux informations et en demander la transcription, par tout traitement approprié, dans des documents directement utilisables pour les besoins du contrôle.

Cependant les nouvelles dispositions viennent préciser que seul un médecin désigné par le Président de la Commission parmi les médecins figurant sur une liste établie par le Conseil de l'Ordre des médecins et comportant au moins cinq noms, peut requérir la communication d'informations

médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins, ou de la gestion de services de santé, et qui est mis en œuvre par un membre d'une profession de santé.

Les contrôles en ligne

L'article 18 de la Loi n° 1.165 vient désormais prévoir explicitement la possibilité pour la Commission d'effectuer des contrôles à distance en permettant aux investigateurs, à partir d'un service de communication au public en ligne, de consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, négligence, ou par le fait d'un tiers, en accédant et en se maintenant dans des systèmes de traitements automatisés d'informations le temps nécessaire aux constatations, et retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

La consécration du contradictoire

Prenant en compte les considérations qui avaient conduit à l'annulation des pouvoirs d'investigation, les modifications législatives intervenues en fin d'année 2015 ont largement introduit le principe du contradictoire lors des opérations d'investigations, mais également après le déroulement de celles-ci.

Ainsi, le nouvel article 18 de la Loi n° 1.165 vient préciser désormais qu'à l'issue des opérations de vérification sur place et sur convocation, un procès-verbal des constatations, vérifications et visites est dressé contradictoirement.

Dans le cadre de cette réforme, le législateur a souhaité modifier l'article 19 de la Loi n° 1.165, relatif aux pouvoirs de sanctions de la Commission, prévoyant également une procédure contradictoire au terme de laquelle lorsque des irrégularités sont constatées, le Président de la CCIN fait établir un rapport notifié au responsable de traitement, lequel dispose d'un délai d'un mois pour formuler ses observations.

A l'issue de cette procédure le Président peut décider d'adresser un avertissement en cas de non-respect des obligations découlant de la Loi n° 1.165, ou une mise en demeure en cas de refus volontaire de mise en conformité, ces deux mesures pouvant être soit alternatives, soit successives.

Si la mise en conformité n'intervient pas dans le délai imparti, le Président de la Commission peut, après avoir invité le responsable de traitement relevant du secteur privé à lui fournir des explications dans un nouveau délai d'un mois, prononcer une injonction de mettre un terme au traitement ou d'en supprimer les effets.

Le Président doit en outre signaler sans délai au Procureur Général les irrégularités constitutives d'infractions pénales, conformément à l'article 19 alinéa 2 de la Loi n° 1.165.

La Commission est de plus habilitée à ester en justice.

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.

De plus, depuis la modification de la Loi n° 1.362 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, intervenue en 2018, ce droit d'accès indirect concerne désormais également les informations traitées par les organismes assujettis à la Loi anti blanchiment, relatives aux obligations de vigilance, de déclaration et d'information auprès du Service d'Information et de Contrôle sur les Circuits Financiers.

Lorsqu'elle est saisie d'une demande de droit d'accès indirect, la Commission ne peut transmettre les informations au demandeur qu'en accord avec le responsable de traitement ou avec le SICCFIN s'il s'agit d'informations détenues par les organismes soumis à la législation relative à la lutte contre le blanchiment de capitaux.

DES SANCTIONS ADMINISTRATIVES

Alors que la CCIN ne disposait d'aucun pouvoir de sanction direct, ce pouvoir, qui lui a été conféré en 2008, constitue le prolongement logique de sa mission de contrôle.

Ainsi 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.

Depuis 2015 les sanctions peuvent être publiées, cependant les mesures de publicité sont susceptibles de faire l'objet d'un recours en cas d'atteinte grave et disproportionnée à la sécurité publique, au respect de la vie privée et familiale ou aux intérêts légitimes des personnes concernées.

LE BUDGET DE LA COMMISSION

Pour l'année 2019 la Commission a disposé d'un budget global de 1.326.300,00 € se répartissant ainsi :

- **776.300,00 € au titre des crédits de fonctionnement ;**
- **550.000,00 € au titre de ses dépenses salariales.**

Par rapport aux années précédentes son budget de fonctionnement a dû être augmenté de 149.000,00 € pour tenir compte des frais liés à ses nouveaux locaux (coût de déménagement, accroissement du montant du loyer, ...).

En 2019 la Commission a en effet été contrainte de déménager du fait d'une opération de réhabilitation qui concerne l'immeuble dans lequel elle avait ses locaux jusqu'alors.

En outre, comme à l'accoutumée une grande partie de son budget de fonctionnement a été consacrée au renforcement de la sécurité de son système d'information par le biais de nouveaux dispositifs destinés à prévenir, détecter et remédier à d'éventuelles intrusions.

De plus les actions de formations de ses Agents ont été poursuivies afin de disposer de compétences de haut niveau dans des domaines pointus et émergents.

L'ORGANISATION DE LA COMMISSION

La Commission se réunit en séance plénière en moyenne au moins une fois par mois pour l'examen des dossiers sur lesquels elle est amenée à formuler un avis ou à délivrer une autorisation. Elle se réunit également de façon extraordinaire lorsque des sujets d'importance le justifient.

Les décisions de la Commission sont adoptées à la majorité des suffrages exprimés, la voix du Président étant prépondérante en cas de partage des voix.

Elle ne peut valablement délibérer que si plus de la moitié de ses membres sont présents.

2

L'ORGANISATION ET LES MISSIONS DU SECRÉTARIAT GÉNÉRAL

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

Après avoir obtenu un diplôme de troisième cycle en droit économique et des affaires, Agnès Lepaulmier Stefanelli débute sa carrière en qualité d'Administrateur au Conseil National puis au Département de l'Intérieur.

En 1997, elle quitte l'Administration pour intégrer la Société Monégasque de l'Electricité et du Gaz où elle occupe les fonctions d'Assistante Juridique puis de Chef du Service Juridique.

En 2013, elle est nommée Directeur Administratif et Juridique de cette Société avant d'intégrer à nouveau l'Administration en septembre 2014 en qualité de Secrétaire Général de la CCIN.

Les années au cours desquelles elle a notamment eu en charge l'accomplissement des formalités résultant de la Loi n° 1.165 lui ont permis de s'imprégner de ce domaine parfois complexe aux enjeux multiples.

Elles lui ont également apporté une vision pratique de la mise en conformité des traitements automatisés d'informations nominatives et des difficultés auxquelles peuvent être confrontés les responsables de traitements lors de l'élaboration de leurs dossiers.

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 quatre 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 ;**
- **d'élaborer les supports d'informations ;**
- **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 dossiers de plaintes ;**
- **d'assurer la représentation de la Commission sur le plan international et de participer aux différents travaux des Autorités étrangères de protection des données ;**
- **d'élaborer les statistiques annuelles de la Commission ;**
- **d'animer des réunions de sensibilisation ;**
- **de vérifier si les déclarations, demandes d'avis ou demandes d'autorisation sont complètes au sens de la Loi n° 1.165.**

En tant que de besoin le Secrétariat Général apporte son assistance et son expertise au Président et aux Membres dans l'accomplissement de leurs missions.

3

LA CCIN AUPRÈS DES INSTITUTIONS ET DES ACTEURS DE LA PRINCIPAUTÉ

A l'occasion de la nomination des Membres de la Commission, SEM Serge TELLE a accueilli les Commissaires ainsi que les Membres du Gouvernement Princier lors d'un déjeuner donné en sa Résidence. Lors de ce déjeuner le Président Guy MAGNAN a indiqué que la Commission nouvellement nommée aura sans nul doute la volonté de poursuivre le dialogue étroit et constructif noué au cours des cinq dernières années avec les entités publiques et privées de la Principauté afin d'accompagner au mieux leur mise en conformité, dans un cadre législatif qui a vocation à évoluer prochainement. Sur ce point la Commission s'est vivement félicitée d'avoir été associée, dès l'origine, aux travaux préparatoires à l'élaboration du projet de Loi destiné à se substituer à la Loi n° 1.165 afin de faire bénéficier la Principauté des plus hauts standards en matière de protection des données personnelles. Ce travail conjoint, initié dès le début de l'année 2018, a en effet permis très utilement à la Commission de faire connaître en amont les grandes orientations qu'il lui semblait pertinent d'introduire dans la nouvelle législation. L'ambitieuse politique gouvernementale du développement du numérique a également été évoquée, ce qui a donné l'occasion aux Membres de la CCIN de rappeler que la concrétisation de ce vaste projet se devait bien évidemment d'être respectueux des droits et libertés de chacun.

Déjeuner donné par SEM le Ministre d'Etat le 17 septembre 2019 à l'occasion de la nomination des Membres de la CCIN

De gauche à droite : M. Arnaud Hamon, Directeur des Affaires Juridiques ; M. Florestan Bellinzona, Commissaire ; Monsieur Marc Vassallo, Secrétaire Général Adjoint du Gouvernement ; Monsieur Didier Gamerdinger, Conseiller de Gouvernement Ministre des Affaires Sociales et de la Santé ; Monsieur Jean-Yves Peglion, Commissaire ; Mme Corinne Laforest de Minotty, Chargée de Mission au Département des Relations Extérieures et de la Coopération ; M. Gilles Tonelli, Conseiller de Gouvernement Ministre des Relations Extérieures et de la Coopération ; Mme Agnès Lepaulmier, Secrétaire Général de la CCIN ; M. Rainier BOISSON, Vice-Président ; SEM Serge Telle, Ministre d'Etat ; M. Guy Magnan, Président ; Mme Marie-Pierre Gramaglia, Conseiller de Gouvernement Ministre de l'Equipement, de l'Environnement et de l'Urbanisme ; M. Jean Castellini, Conseiller de Gouvernement Ministre des Finances et de l'Economie ; M. Philippe Blanchi, Commissaire ; Monsieur Patrice Cellario, Conseiller de Gouvernement Ministre de l'Intérieur ; M. Jean-François Cullieyrier, Commissaire.

Le souhait de poursuivre l'accompagnement des entités de la Place s'est une nouvelle fois traduit au cours de l'année 2019 par de nombreuses réunions destinées à appréhender en amont la protection des informations nominatives.

Ainsi, dans le cadre de l'application des modifications législations intervenues en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, des réunions ont été organisées avec le SICCFIN afin d'évoquer le nouvel outil métier dont il doit se doter pour recevoir de manière dématérialisée les déclarations de soupçon et adresser des demandes de renseignements aux organismes assujettis à cette législation. De plus, à l'occasion de la nomination du nouveau Directeur du SICCFIN, des réunions ont utilement permis d'évoquer les questions de la protection des données communes à ces deux régulateurs, dans la perspective de l'éventuelle publication conjointe de textes d'orientation à vocation générale. Ces échanges ont également porté sur les missions de la CCIN en matière d'exercice, par les personnes concernées, d'un droit d'accès indirect aux informations les concernant qui seraient détenues par des établissements bancaires ou par le SICCFIN ; ainsi que sur les contours exacts du champ d'application des vérifications à effectuer au titre de la lutte contre le blanchiment de capitaux.

De nombreuses réunions ont eu lieu avec les Services de l'Etat concernant les deux projets de Loi relatifs d'une part à l'identité numérique, et d'autre part à l'économie numérique dont la Commission a été saisie pour avis, au mois de mars.

Ces échanges ont eu pour objectif premier d'avoir une vision plus précise des ambitions du Gouvernement en matière de développement du numérique en Principauté. Ainsi le 17 juillet 2019, Monsieur Frédéric GENTA, Délégué Interministériel en charge de la Transition Numérique, a présenté à la Commission les considérants qui sous-tendent la volonté du Gouvernement Princier de développer l'usage du numérique, ainsi que les nombreux projets envisagés par les Services de l'Etat dans des domaines aussi variés que l'économie, la santé, l'éducation, les relations Administration / administrés, la smart city, ... La Commission a parfaitement perçu les enjeux du développement du numérique à Monaco. Cependant elle a souligné que ses points d'attention, dans le strict respect du cadre de ses missions, concernent bien évidemment la sécurité des données liées à l'identité numérique, l'identification des données qui seront nécessaires à la création d'une identité / identifiant numérique et la maîtrise des accès auxdites données, ainsi que la facilité d'utilisation, pour les usagers, de cette identité numérique et des services qui y seront associés.

De gauche à droite : Messieurs PEGLION, CULLIEYRIER, BLANCHI, Commissaires, Monsieur BOISSON, Vice-Président de la CCIN, Monsieur GENTA, Délégué Interministériel en charge de la Transition Numérique, Monsieur MAGNAN, Président de la CCIN, Monsieur BELLINZONA, Commissaire.

Parallèlement à ces échanges avec les Services Gouvernementaux, un dialogue fructueux s'est noué avec le Conseil National, par le biais de Monsieur Franck JULIEN, Président de la Commission pour le Développement du Numérique, qui a participé à plusieurs réunions de travail avec les Services de la CCIN afin d'échanger sur la version initiale des projets de Loi, que la Haute Assemblée souhaitait également enrichir de nombreux amendements afin d'en préciser les notions et les contours. A l'issue de ces réunions de travail une délégation de la CCIN a pu utilement échanger avec les Membres de la Commission pour le Développement du Numérique afin d'évoquer plus particulièrement le contenu du « *registre national* », les distinctions entre « *identité* » et « *identifiant* » numériques, et les préoccupations communes relatives à la nécessité que les projets de Loi initiaux soient enrichis afin d'en faciliter la compréhension et donc l'application.

Par ailleurs l'année 2019 a été mise à profit afin d'évoquer avec Monsieur Patrice CELLARIO, Conseiller de Gouvernement Ministre de l'Intérieur et la Direction de la Sûreté Publique (DSP) le fondement juridique qui serait nécessaire à la mise en œuvre, par la DSP, de traitements particulièrement intrusifs au regard des droits des personnes, afin de déterminer si les dispositions de la Loi n° 1.430 portant diverses mesures relatives à la préservation de la sécurité nationale constituaient, en l'état, un cadre suffisamment clair et précis. Sur ce point la Commission a pris connaissance avec satisfaction des déclarations gouvernementales faites en séance publique du Conseil National le 12 décembre 2019. En effet, après que la Haute Assemblée ait, de manière unanime, souligné que l'utilisation d'un dispositif de reconnaissance faciale associé à l'exploitation des caméras de vidéoprotection urbaine ne pouvait être envisagée qu'après un débat avec les élus dans le cadre de l'examen de dispositions législatives, le Gouvernement a affirmé publiquement que le

recours éventuel à ce type de technologie ne se ferait qu'après le vote de dispositions légales. Les représentants du Gouvernement ont également fait part des échanges intervenus avec la CCIN, au terme desquels la décision a été prise par les Services de l'Etat de procéder par voie législative et non réglementaire.

Des échanges avec la DSP ont également eu lieu plus particulièrement avec les Agents de la Cellule nouvellement créée de lutte contre la cybercriminalité. En effet, au regard de la nature des plaintes dont la DSP est saisie en matière d'usurpation d'identité sur les réseaux sociaux, les actions de la CCIN menées directement auprès des administrateurs de ces réseaux conduisent rapidement à remédier à ces situations qui peuvent s'avérer extrêmement préjudiciables pour les victimes.

En milieu d'année des réunions ont été initiées avec l'Institut Monégasque de la Statistique et des Etudes Economiques (IMSEE) et Madame la Déléguée pour la Promotion et la Protection des Droits des Femmes afin d'évoquer les modalités de réalisation d'une nouvelle enquête relative aux violences faites aux femmes. L'objectif était ici de garantir une stricte anonymisation des données transmises à l'IMSEE par les différentes entités amenées à traiter la situation des victimes (CHPG, DSP, Association d'Aide aux Victimes d'Infractions Pénales, les Services Judiciaires ou encore la Direction de l'Action et de l'Aide Sociales) tout en évitant qu'un même cas soit comptabilisé plusieurs fois. Les échanges avec l'IMSEE ont également concerné les modalités de réalisation de l'enquête sur l'égalité salariale, et de la transmission des données anonymisées par la Caisse de Compensation des Services Sociaux.

Afin d'accompagner le développement de l'usage du numérique en matière médicale les Services de la Commission ont été conviés à l'initiative de Monsieur le Conseiller de Gouvernement Ministre des Affaires Sociales et de la Santé, à une réunion tenue dans les locaux de la Délégation française aux Affaires Européennes et Internationales en présence des représentants des Autorités françaises, dans la perspective de déployer, en Principauté, le Dossier Médical Partagé (DMP). L'objectif de cette réunion était d'envisager les instruments juridiques ainsi que les modalités techniques à mettre en œuvre afin que le DMP monégasque soit interopérable avec le DMP français, le but étant l'exhaustivité des données de santé des patients consultant en France et en Principauté. S'agissant plus particulièrement du volet relatif à la protection des données personnelles, il a été convenu de poursuivre les discussions afin de déterminer le cadre juridique le plus approprié permettant l'alimentation du DMP à

partir d'informations nominatives en provenance tout à la fois de la France et de Monaco. A l'issue de ces premiers échanges il a été convenu de continuer à œuvrer conjointement à la mise en œuvre du dossier médical partagé au-delà des frontières, au travers de groupes de travail franco-monégasques thématiques.

Comme à l'accoutumée, des réunions ont été également organisées avec Monaco Telecom afin d'exposer aux Services de la CCIN les projets en cours, avant dépôt officiel des demandes d'avis correspondantes. Ont ainsi été évoqués « *Monaco Care Safety* », qui est une protection multi-équipements contre les menaces de l'Internet, « *Monaco Care Password* », permettant la gestion de mots de passe multi-équipements, l'application de suivi de consommation mobile mise à disposition des clients, ou encore la gestion du service de télévision sur IP.

Au cours de l'année écoulée les réunions trimestrielles avec l'Association Monégasque des Activités Financières (AMAF) se sont poursuivies et ont notamment eu pour objet les modalités d'application des obligations issues du RGPD, auquel de nombreux établissements situés à Monaco sont soumis (formation, désignation et localisation du DPO, ...).

L'application des nouvelles dispositions en matière de LAB, ainsi que l'état d'avancement des travaux sur la modification de la Loi n° 1.165, ou encore la question de l'accès extraterritorial aux données de la clientèle, ainsi que le traitement des données nominatives à l'occasion des prestations de service externalisées ont également été évoqués.

Si l'AMAF est un relai utile dans la remontée de problématiques communes à l'ensemble des entités bancaires et financières de la Place, de nombreuses réunions se sont également tenues avec des établissements qui désiraient exposer aux Services de la CCIN leur organisation spécifique et les politiques souhaitées par leur société mère ou du siège afin d'évoquer les échanges d'informations qu'il est envisageable d'effectuer, ou non, dans un contexte où les partages de données nominatives entre entités d'un même groupe ont tendance à se multiplier.

Par ailleurs, en fin d'année, à l'invitation du bureau du Conseil de l'Ordre des Experts Comptables, les Services de la Commission ont effectué une présentation à la profession afin d'évoquer les principales exigences du RGPD auquel de nombreuses entités de la Principauté sont soumises dans la mesure où elles offrent des biens ou des services à des personnes situées sur le territoire de l'Union européenne.

4

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.

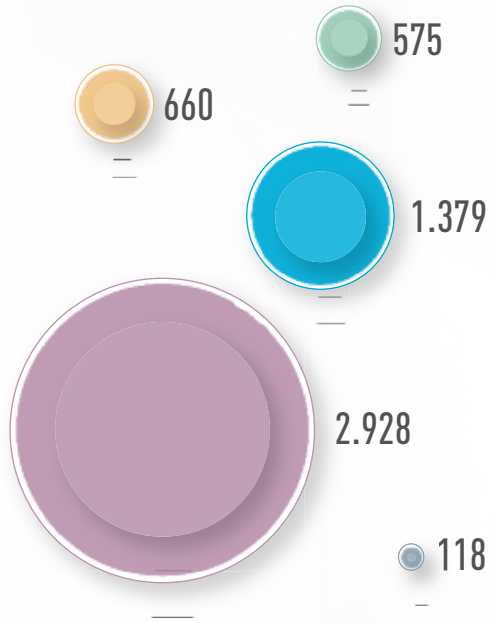
Il peut être consulté au siège de la Commission par toute personne physique ou morale souhaitant s'assurer de l'existence légale d'un traitement automatisé d'informations nominatives.

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 2019

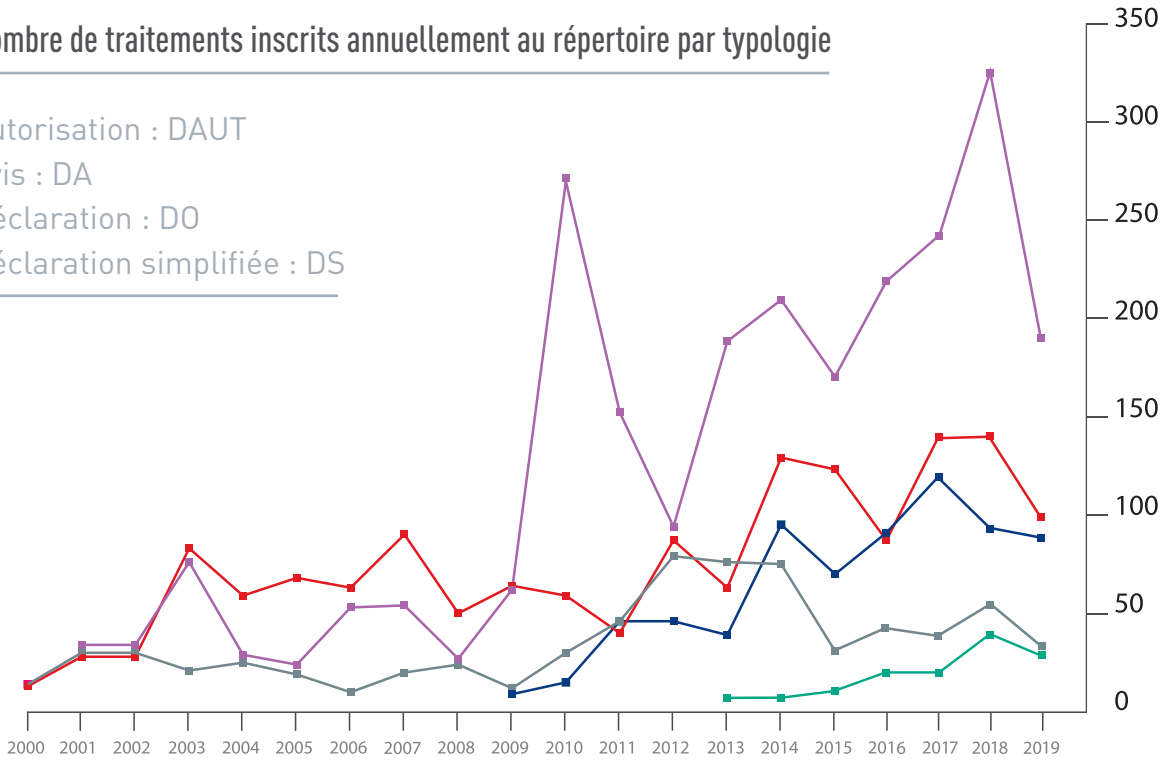
5.660 se répartissant ainsi :

- **575** traitements du secteur public ou assimilé
- **660** traitements ayant fait l'objet d'une autorisation de la Commission
- **1.379** traitements ayant fait l'objet d'une déclaration ordinaire
- **2.928** traitements ayant fait l'objet d'une déclaration simplifiée
- **118** 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
DS		26	26	68	21	16	45	46	19	54	856	144	86	180	201	162	221	243	326	188
DO	5	20	20	75	51	60	55	82	42	56	51	32	79	55	121	115	81	140	141	98
DA	6	22	22	13	17	11	2	12	16	4	22	38	71	68	67	23	34	38	54	35
DAUT								1		1	7	38	38	31	87	62	89	119	90	97
TRANSFERT														1	1	4	21	21	41	29

Nombre de nouveaux traitements inscrits au répertoire en 2019

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

188

traitements ayant fait l'objet d'une déclaration simplifiée

97

TRAITEMENTS DONT LA MISE EN ŒUVRE A ÉTÉ AUTORISÉE PAR LA COMMISSION

98

traitements ayant fait l'objet d'une déclaration ordinaire

35

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

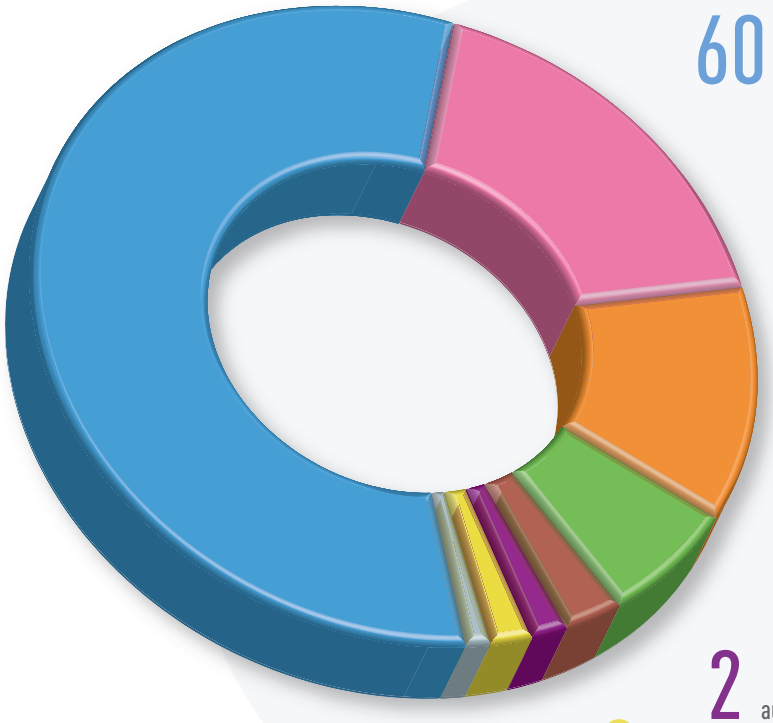
29

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

Nombre de délibérations rendues par la Commission en 2019

Au cours de l'année écoulée, la Commission a rendu 206 délibérations se répartissant ainsi :

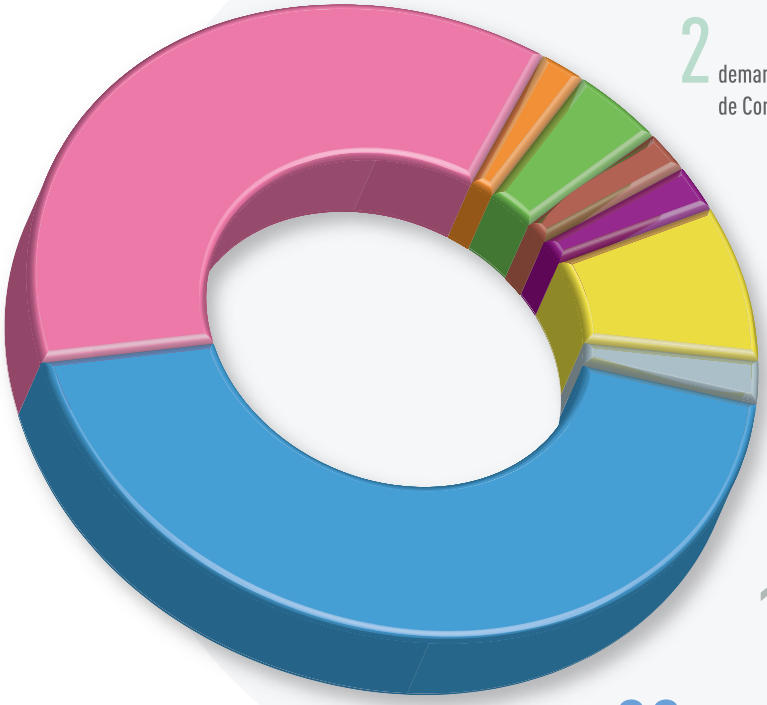
107 autorisant la mise en œuvre ou la modification de traitements :



- **60** autorisations relatives à des dispositifs de vidéosurveillance
- **19** autorisations relatives aux traitements concernant plus spécifiquement le secteur bancaire et assimilé
- **13** autorisations relatives à des dispositifs de contrôle d'accès biométriques ou non
- **7** autorisations relatives aux enregistrements téléphoniques
- **3** autorisations relatives à la messagerie électronique
- **2** autorisation relative aux alertes professionnelles
- **2** autorisations relatives aux habilitations
- **1** autorisation relative à l'analyse des performances des salariés

3 portant refus d'autorisation

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



18 demandes d'avis présentées par le CHPG

1 demande d'avis présentée par la Société Monégasque de l'Electricité et du Gaz

2 demandes d'avis présentées par la Commission de Contrôle des Informations Nominatives

1 demande d'avis présentée par le Conseil National

1 demande d'avis présentée par la CAMTI CARTI

4 demandes d'avis présentées par de Monaco Telecom

1 demande d'avis présentée par la Société Monégasque des Eaux

22 demandes d'avis présentées par le Ministre d'Etat

3 Portant avis défavorable	**4** Portant sur une mission d'investigation
28 Autorisant un transfert d'informations nominatives vers un Pays ne disposant pas d'un niveau de protection adéquat : la plus grande partie a concerné le secteur bancaire	**2** Portant recommandation
	4 Portant décision sur les délais de conservation des informations nominatives prévus par déclaration ordinaire
4 Portant avis sur des projets de textes transmis par le Ministre d'Etat	**1** Relative au fonctionnement interne de la CCIN

5

LA CCIN ET LES DROITS DES PERSONNES CONCERNÉES

LES CONSULTATIONS DU RÉPERTOIRE PUBLIC DES TRAITEMENTS

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

Les informations figurant dans ledit répertoire sont les suivantes :

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

Au cours de l'année 2019 ce répertoire a été consulté 3 fois, par des Cabinets conseils 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 la mise en conformité.

De plus, pour les entités de la Principauté soumises au RGPD, la consultation du répertoire des traitements sert également de base à l'élaboration du registre des traitements, si celle-ci leur est imposée.

LES PLAINTES

24 plaintes ont été adressées à la Commission en 2019, en forte augmentation par rapport à l'année précédente au cours de laquelle la CCIN avait été saisie par 15 plaignants.

Cette forte augmentation résulte d'une meilleure sensibilisation des personnes concernées au respect de leurs droits, et à leur souhait d'accroitre la maitrise de leurs données à caractère personnel.

La défense des droits des personnes concernées

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.

Le droit d'accès

Saisie sur le fondement de ce droit d'accès, la Commission a eu à connaître d'une plainte émanant d'un ancien athlète de haut niveau, qui rencontrait des difficultés pour obtenir l'intégralité des informations le concernant de la part d'une fédération sportive. En dépit de plusieurs démarches effectuées par son Avocat directement auprès de l'organisme en cause, la totalité des informations souhaitées, qui pour certaines dataient de près de 20 ans, n'avait pu être obtenue. En réponse

à l'intervention de la CCIN, il lui a été indiqué que les informations souhaitées avaient été transmises et que le caractère tardif de cette communication s'expliquait par la nécessité de procéder aux vérifications relatives à la qualité de la personne effectuant la demande, au regard de la sensibilité des informations dont la communication était demandée.

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.

15 plaintes ont été reçues en 2019 concernant le droit de suppression, qui a constitué le domaine pour lequel la CCIN a été saisie le plus souvent.

Le droit de suppression

- 10 plaintes ont concerné des demandes de suppression d'informations accessibles sur le net.

La première plainte n'a donné lieu à aucune intervention de la CCIN dans la mesure où il lui a été demandé de faire supprimer un catalogue en ligne de vente aux enchères dans lequel figurait un portrait d'une personne décédée qui avait à l'époque servi de modèle à un peintre. Après instruction de cette plainte il est en fait apparu que les héritiers de la personne décédée souhaitaient faire annuler la mise aux enchères de ce portrait.

Une autre plainte a concerné une ancienne salariée qui, alors qu'elle avait quitté depuis plusieurs mois la société qui l'employait précédemment, avait constaté que sa photo et ses coordonnées figuraient toujours sur le site Internet de son ex employeur. L'intervention de la CCIN a permis une suppression rapide de ces informations qui n'étaient plus d'actualité. Concernant la diffusion de photos sur Internet ou sur les réseaux sociaux, il a été également rappelé que l'accord exprès des personnes concernées était une condition essentielle préalable à une telle diffusion.

Deux demandes de suppression ont également été effectuées auprès respectivement de Google et de Facebook, concernant des propos que les personnes concernées estimaient diffamatoires.

- Dans le premier cas seul le déréférencement de l'article à partir des recherches effectuées sur le nom du mari de la plaignante a été obtenu, Google considérant que la demanderesse avait joué un rôle particulier dans la vie publique et que l'accessibilité des informations concernées était justifiée par l'intérêt du public à en connaître.
- Le second cas a concerné une demande de suppression de propos publiés sur une page Facebook et laissant à penser que le plaignant avait dérobé des œuvres d'art. De plus des commentaires portaient également sur sa vie privée. Facebook a ici fait valoir que les propos en question n'étaient pas diffamatoires.

Face à ces deux refus de nouvelles demandes ont été introduites par la CCIN afin d'obtenir les suppressions souhaitées.

Trois plaintes ont concerné la publication, par un site Internet hébergé aux Etats-Unis, des identités et des coordonnées (adresse et numéro de téléphone personnels) de personnes résidant en Principauté, sans aucun accord de leur part, et sans qu'elles en aient été préalablement informées. Après plusieurs démarches la CCIN a pu obtenir la suppression des informations concernées.

La CCIN a également été saisie d'une demande d'une personne ayant fait l'objet d'une mesure de gel de fonds qui a pris fin en 2018. Toutefois les recherches effectuées dans les moteurs de recherches à partir du nom de la plaignante renvoyaient sur l'Arrêté Ministériel ayant prononcé cette mesure. Une réunion avec les différents Services de l'Etat a permis d'acter la nécessité qui s'attachait à ne plus rendre accessible cet Arrêté Ministériel à partir du nom de l'intéressée, et les mesures techniques y afférentes ont été mises en place rapidement.

Par ailleurs deux saisines ont émané de personnes morales :

- Une société de vente de véhicules suite à la création d'une page Facebook frauduleuse à son nom invitant les internautes à laisser leurs coordonnées afin de recevoir la livraison d'une voiture qu'ils auraient prétendument gagnée. Peu de jours après la réception de cette plainte la page Facebook en cause avait déjà été supprimée.
- Une société de prestation de services suite à un commentaire défavorable publié sur sa page Google My Business, émanant d'une personne avec laquelle la plaignante n'avait jamais été en contact. Les démarches auprès de Google My Business n'ont pas abouti à faire supprimer ce commentaire au motif « *qu'il ne présente pas de caractère manifestement illicite et ne dépasse pas le cadre légal de la libre critique* ». La CCIN a toutefois conseillé au plaignant de poster un commentaire en réponse, indiquant que l'auteur de commentaire était inconnu et ne figurait pas parmi ses clients.

S'agissant des personnes morales, il est à noter que la Loi n° 1.165 relative à la protection des informations nominatives leur offre un certain niveau de protection.

Ainsi conformément à l'article 13 de ladite Loi :

« *Toute personne morale a le droit :*

- *de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement, sauf le cas où celui-ci est mis en œuvre, dans le cadre exclusif de leurs missions d'intérêt général, par les responsables de traitements visés à l'article 7 [autorités publiques, organismes de droit privé investis d'une mission d'intérêt général, ...] ;*
- *d'accéder, dans les conditions prévues à la section II, aux informations la concernant ou, avec l'accord de ses membres, d'accéder aux informations nominatives les concernant, et d'obtenir qu'elles soient modifiées s'il y a lieu* ».

Toutefois les droits conférés actuellement aux personnes morales par la législation interne au titre de la protection des informations nominatives ne se retrouvent pas dans les standards européens régissant la matière, et devraient sans doute évoluer à court terme dans le droit monégasque.

Cette spécificité rend de plus en plus difficiles les interventions de la CCIN lorsqu'elle n'est pas saisie par une personne physique.

- 3 plaintes ont concerné des demandes de suppression de liste de diffusion d'emails :

Dans ces saisines les plaignants ne voulaient plus recevoir de courriels calomnieux portant sur plusieurs personnalités de Monaco et, malgré leurs tentatives, ne parvenaient pas à faire retirer leur adresse email de la liste de diffusion.

Il est toutefois apparu que la personne qui envoyait ces communications avait une adresse professionnelle hors de la Principauté, ce qui n'a pas permis à la CCIN d'intervenir auprès d'elle.

De plus la CCIN a été saisie par :

- Une personne qui était pressentie pour intégrer le bureau d'une Association et qui a rencontré des difficultés afin d'obtenir confirmation que les informations nominatives la concernant avaient bien étaient supprimées des traitements de ladite Association, son projet d'en devenir Membre n'ayant pas abouti.
- Un ancien salarié qui a constaté que son adresse nominative de messagerie professionnelle n'avait pas été désactivée après son départ et était utilisée par un autre salarié.

Dans ces deux cas l'intervention de la CCIN a permis une résolution rapide des différends.

Par ailleurs au cours de l'année écoulée 8 plaintes ont concerné l'exploitation des traitements automatisés d'informations nominatives.

L'exploitation des traitements automatisés d'informations nominatives

La vidéosurveillance

Toujours au cœur des préoccupations des personnes concernées, 3 plaintes ont porté sur des dispositifs de vidéosurveillance exploités respectivement dans un restaurant, une boutique et un immeuble d'habitation.

Dans le premier cas un riverain craignait que le dispositif permette de filmer ses allées et venues, ce qui, après instruction du dossier, s'est révélé ne pas être le cas.

Dans le deuxième le Président de la Commission a rappelé au responsable de traitement les obligations légales en matière d'exploitation d'un système de vidéosurveillance, à savoir l'obligation d'obtention d'une autorisation du Ministre d'Etat puis de la CCIN.

Concernant les caméras au sein d'un immeuble d'habitation, des résidents ont cru qu'une nouvelle caméra récemment installée permettait de filmer leur terrasse privative. L'instruction du dossier a permis de constater que tel n'était pas le cas.

Les traitements spécifiques à certaines professions

2 plaintes ont concerné l'application par les établissements bancaires et assimilés des réglementations relatives d'une part à l'échange automatique d'information en matière fiscale, et d'autre part à MIFID II au titre des transactions sur instruments financiers sur les marchés situés en Union européenne. Après examen des réglementations spécifiques applicables à ces domaines, la CCIN est revenue vers les plaignants afin de leur préciser les dispositions applicables, qui fondent la collecte et le traitement des données des clients par les établissements teneurs de leurs comptes.

Par ailleurs, dans le prolongement de plaintes reçues l'année précédente, la CCIN a une nouvelle fois été saisie par 2 conducteurs de taxis concernant le dispositif de gestion des courses dont la mise en œuvre a fait l'objet d'un avis favorable de la Commission en 2018. Les plaintes concernaient à nouveau le fait que la localisation de tous les taxis pouvait être accessible par chacun d'eux. Les échanges avec le responsable de traitement ont fait apparaître que les modifications de l'applicatif, qui avaient été initiées quelques mois auparavant, ne permettaient plus au prestataire en charge de la gestion des courses de taxis de connaître leur statut (libre, en station, indisponible,...) ce qui n'était pas satisfaisant. Les assurances ont été données à la Commission que le problème allait être résolu dans les plus brefs délais.

La sécurisation de l'exploitation des données

Il est de pratique de plus en plus courante que les établissements effectuant des analyses ou des examens médicaux mettent les résultats et comptes rendus à disposition des patients par le biais de dispositifs numériques. Si ceux-ci sont dûment sécurisés, la CCIN a cependant reçu une plainte d'un patient qui, ayant perdu ses identifiants lui permettant d'accéder à ses résultats d'examen, a pu les obtenir à nouveau par le simple fait de se présenter au comptoir d'accueil de l'établissement concerné et de décliner son identité, sans avoir à produire un document attestant de celle-ci.

Compte tenu de la nature particulièrement sensible des données concernées, la CCIN est intervenue sur le champ auprès du responsable de traitement afin de l'alerter sur les conséquences d'un tel défaut de vérification, permettant potentiellement à des personnes non autorisées d'accéder à des données de santé. L'établissement en cause a immédiatement mis en place une procédure aux fins de s'assurer que toute personne demandant des identifiants de connexion soit habilitée à accéder aux données.

LES SANCTIONS

En application de l'article 19 de la Loi n° 1.165, le Président de la Commission a adressé en 2019 une mise en demeure de désactiver sur le champ un dispositif de vidéosurveillance exploité de manière illégale.

Cette sanction a fait suite à un contrôle sur place réalisé en fin d'année 2018, et a été motivée par :

- l'irrégularité de la mise en œuvre du dispositif de vidéosurveillance, et la poursuite de son utilisation alors que le responsable de traitement ne pouvait ignorer le caractère illicite celle-ci en l'absence de l'autorisation délivrée par la CCIN ;
- l'implantation des caméras dont certaines filmaient de manière permanente des salariés à leur poste de travail sans aucune justification particulière (caisse, ou manipulation d'objets précieux par exemple) ;
- l'utilisation des images des caméras de vidéosurveillance : il a été constaté que le dispositif servait à vérifier les heures d'arrivée des salariés notamment par le biais d'accès distants ouverts par les dirigeants. Il servait également à donner des instructions en temps réel et à distance aux salariés, conduisant à une surveillance permanente et inopportune de ceux-ci ;
- le défaut de mesures de sécurisation des accès au dispositif de vidéosurveillance et aux images ;
- le défaut d'information préalable des personnes concernées (aucun pictogramme aux entrées des établissements notamment).

De plus lors du contrôle, l'un des dirigeants a tenté de soustraire des éléments aux Agents contrôleurs en essayant de dissimuler des documents figurant dans le dossier d'un salarié, et prouvant que les caméras étaient utilisées à des fins de contrôle des horaires de travail.

Les relations avec le Parquet Général

Sur le fondement de l'article 19 de la Loi n° 1.165 au terme duquel les irrégularités à la législation relative à la protection des informations nominatives sont signalées au Procureur Général, le Président de la Commission a, en 2019, transmis un dossier au Parquet.

Cette transmission a concerné le dossier pour lequel une mise en demeure de désactiver le dispositif de vidéosurveillance a été adressée de manière concomitante au responsable de traitement (cf supra).

En effet, considérant les nombreuses irrégularités qui ont été constatées lors des opérations de contrôle, et prenant en compte la tentative de

soustraire des éléments aux Agents contrôleurs, le Président a souhaité saisir le Parquet de cette affaire.

Cette saisine s'est effectuée notamment sur le fondement de l'article 22-3° de la Loi n° 1.165 aux termes duquel :

« *Sont punis d'un emprisonnement de trois mois à un an et de l'amende prévue au chiffre 4 de l'article 26 du code pénal ou de l'une de ces deux peines seulement :*
(...)
3° ceux qui volontairement empêchent ou entravent les investigations opérées pour l'application de la loi ou ne fournissent pas les renseignements ou documents demandés ».

Cette transmission au Procureur Général a donné lieu à des échanges courant 2019 avec la Direction de la Sûreté Publique afin de savoir si le dispositif de vidéosurveillance en cause avait en définitive obtenu une autorisation de mise en œuvre de la part de la CCIN.

LES INVESTIGATIONS

Les contrôles sur place

Deux contrôles sur place ont été effectués en 2019 et ont concerné tous les deux un dispositif de vidéosurveillance.

Ces deux contrôles ont été réalisés sur autorisation du Président du Tribunal de Première Instance.

Le premier a fait suite à une plainte relative à l'éventuel accès distant par la Direction à un dispositif de caméras, qui aurait pu permettre à l'insu des personnels un contrôle permanent et inopportun de ces derniers. Ledit dispositif était légalement mis en œuvre et avait été préalablement autorisé par la CCIN sans qu'aucun accès distant n'ait été mentionné au dossier. Afin d'analyser la conformité du dispositif, deux vérifications sur place, et une vérification sur pièces, faisant également intervenir les prestataires du responsable de traitement ont été réalisées.

Le contrôle a mis en exergue qu'un accès distant était effectivement techniquement possible du fait du recours à une box Internet affectée au système de vidéosurveillance pour le transit des données entre le local technique et le local de vidéosurveillance. Le défaut constaté s'analysait plus en un défaut de sécurité qu'en une volonté de surveiller les salariés. La sécurité du traitement a par la suite été mise aux normes.

Le second contrôle sur place a fait suite à un signalement selon lequel des caméras étaient installées dans les sanitaires d'un restaurant. Dès la première visite des Agents contrôleurs les caméras qui étaient installées dans les vestibules d'accès aux sanitaires ont été immédiatement déposées.

Une campagne d'investigation en ligne

Au mois de mai 2019 la Commission a souhaité lancer une campagne d'investigation en ligne concernant 10 sites Internet.

Ce souhait résultait du constat de la multiplication des fonctionnalités des sites Internet (achats de biens ou de services, accès à des résultats médicaux, ...) du développement des outils de mesures d'audience et de traçage, et de la méconnaissance, par de nombreux responsables de traitement, des règles régissant ce domaine.

Le panel choisi pour ces contrôles s'est voulu représentatif des fonctionnalités offertes par les sites internet et de leurs acteurs : site purement institutionnel de présentation, site marchand, ...

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.

Les contrôles opérés ont permis de constater dans la majeure partie des cas un défaut de maîtrise, voire de connaissance, des outils installés sur les sites Internet.

Les échanges intervenus avec les responsables de traitements et leurs prestataires ont eu vocation à les alerter sur les fonctionnalités, les transferts de données opérés par certains outils utilisés, et la qualité de l'information qu'ils doivent à leurs clients, notamment s'il convient de recueillir le consentement de ces derniers pour le déploiement de certaines fonctionnalités.

Il a par ailleurs été constaté que les mesures de sécurité entourant la mise à disposition des Internautes de données sensibles (résultats médicaux par exemple) étaient la plupart du temps bien maîtrisées, de même que les dispositifs mis en place en matière de vente en ligne.

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.

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

C'est dans ce cadre qu'au cours de l'année 2019 il a été procédé à 5 vérifications : 2 auprès de la Direction de la Sûreté Publique et 3 auprès du Service d'Information et de Contrôle sur les Circuits Financiers.

Une vérification auprès de la DSP a permis de constater que le dossier du requérant n'avait pas été mis à jour d'une décision de réhabilitation prononcée en 2013 par la Chambre du Conseil de la Cour d'Appel Correctionnelle, faisant suite à une condamnation intervenue en 2007 alors que le requérant était mineur.

Le second dossier a nécessité une vérification concomitante auprès de la DSP et du SICCFIN, et se poursuivra en 2020 par deux vérifications auprès d'établissements bancaires.

En effet, depuis les modifications intervenues au mois de juin 2018 en matière de lutte contre le blanchiment de capitaux, les droits d'accès indirects peuvent également s'exercer auprès des organismes assujettis à la législation y afférente.

Les deux autres vérifications effectuées en 2019 auprès du SICCFIN ont concerné des difficultés que rencontraient les personnes concernées pour ouvrir un compte bancaire, et ont été l'occasion de revenir sur les durées de conservation des informations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, telles que modifiées en juin 2018.

Par ailleurs en 2019, faisant suite à un droit d'accès indirect exercé en toute fin d'année 2018 auprès de la Direction de la Sûreté Publique, des informations contenues dans le dossier de la requérante ont été supprimées, car dépourvues de tout lien avec la finalité initiale pour laquelle elles avaient été collectées.

UNE CONDAMNATION POUR NON-RESPECT DU DROIT D'ACCÈS

En fin d'année 2015 le Président de la CCIN avait été saisi par un salarié des difficultés qu'il rencontrait à obtenir des données de pointage de la part de son employeur.

Après plusieurs démarches infructueuses auprès du responsable de traitement, le dossier avait été transmis au Procureur Général pour non-respect des dispositions relatives à la communication des informations suite à une demande de droit d'accès direct.

Par décision en date du 19 mars 2019 le Tribunal Correctionnel, après avoir relevé qu'en dépit des démarches de la CCIN et de la procédure par devant le juge des référés du Tribunal du Travail le plaignant n'avait pu obtenir ses données nominatives de pointage, a condamné l'ancien employeur au paiement de 18.000,00 euros d'amende et au versement de 15.000,00 euros de dommages et intérêts.

LES DOSSIERS DU SECTEUR PUBLIC ET ASSIMILÉ

6

LA POURSUITE DE LA MISE EN ŒUVRE DE L'ÉCHANGE AUTOMATIQUE D'INFORMATIONS À DES FINS FISCALES

Dans le prolongement de ses travaux menés en 2017 et 2018 consacrés aux échanges automatiques d'informations à des fins fiscales, la Commission a adopté trois nouvelles délibérations au mois d'avril 2019.

La première a concerné la mise en œuvre du traitement destiné à gérer les accès à la plateforme dédiée au dépôt des déclarations effectuées pays par pays, dans le cadre de l'action 13 du BEPS, prévue par l'article 3 de l'Ordonnance Souveraine n° 6.713 du 14 décembre 2017 portant application de l'Accord multilatéral entre autorités compétentes portant sur l'échange des déclarations pays par pays. Au terme de ces dispositions : « *toute Entité déclarante, résidente fiscale de Monaco, est tenue de transmettre à la Direction des services fiscaux une Déclaration pays par pays portant sur son exercice fiscal déclarable conformément aux dispositions des articles 5 et 6* » dans les délais mentionnés à l'article 4 de celle-ci.

La Commission a observé que le traitement avait pour objectif d'ajouter une fonctionnalité au téléservice mis en œuvre par la Direction des Services Fiscaux permettant aux Entités déclarantes d'effectuer la déclaration pays par pays.

Elle a relevé que, conformément à ses recommandations, la collecte des copies des documents officiels (carte d'identité ou passeport) destinée à identifier les personnes effectuant ces déclarations s'effectuait en noir et blanc, barré, et a vérifié que les informations collectées étaient adéquates, pertinentes et non excessives au regard de la finalité du traitement soumis.

Par délibération n° 2019-53 elle a de plus émis un avis favorable relatif au traitement destiné à gérer les échanges spontanés de renseignements à des fins fiscales dans le cadre de l'action 5 du BEPS. Sont concernés par ce traitement les Agents habilités de la Direction des Services Fiscaux et les personnes physiques concernées par un Tax-Rulling défini comme « *une prise de position formelle de l'administration fiscale saisie par un contribuable. Elle peut être à l'attention d'une personne physique, une société ou une transaction et pour une durée définie* ».

A l'examen de ce dossier la Commission a pris acte que les informations étaient susceptibles d'être communiquées à des fins fiscales, au travers de la plateforme d'échange automatique d'informations :

- aux autorités compétentes des juridictions du cadre inclusif BEPS ;
- à des juridictions soumises à déclaration situées dans des pays ne disposant pas d'un niveau de protection adéquat au sens de la Loi n° 1.165 du 23 décembre 1993.

A cet égard, elle a précisé que la licéité des communications d'informations nominatives vers des pays ne disposant pas d'un niveau de protection adéquat serait analysée dans la demande d'autorisation de transfert concomitamment soumise.

Ainsi, par délibération n° 2019-054 également en date du 17 avril 2019 elle a autorisé le transfert d'informations nominatives y afférent en relevant que ledit transfert avait pour objet de respecter les engagements de la Principauté envers l'OCDE au titre de l'échange automatique d'informations en matière fiscale.

Elle a toutefois constaté que la liste des juridictions entrant dans le cadre inclusif du BEPS, destinataires des informations nominatives en objet, était susceptible d'évoluer, et a de ce fait demandé que chaque modification de cette liste soit portée à sa connaissance.

L'UTILISATION DE LA LISTE ÉLECTORALE POUR LA COMMUNICATION INSTITUTIONNELLE OU POLITIQUE DU CONSEIL NATIONAL

Afin de pouvoir communiquer aux personnes de nationalité monégasque des informations sur l'actualité institutionnelle ou politique du Conseil National, le Président de la Haute Assemblée a soumis à la CCIN une demande d'avis visant à utiliser à cette fin la liste électorale.

Dans le cadre de l'examen de ce dossier la Commission a relevé qu'aux termes de l'article 6 de la Loi n° 839 du 23 février 1968 sur les élections nationales et communales « *Toute personne de nationalité monégasque peut, à tout moment, prendre communication et obtenir sans frais copie de la liste électorale, sur support papier ou sous format électronique, à la condition de s'engager à ne pas en faire un usage contraire aux dispositions de l'article 80 bis* ».

Sur ce point elle a noté que la demande de communication de la liste électorale sera effectuée annuellement par le Président du Conseil National qui en fera la demande à titre personnel « *en vue d'un usage politique fait par l'Institution qu'il représente* ».

De plus, en application de l'article 80 bis de la Loi n° 839 « *L'utilisation d'une ou plusieurs indications nominatives extraites de la liste électorale n'est autorisée qu'aux seules fins de communication politique, électorale ou institutionnelle ou encore en application d'une disposition législative ou réglementaire, y compris en dehors des périodes de campagne électorale (...)* ».

La Commission a en outre pris acte que l'article 34 de la Loi n° 771 du 25 juillet 1964 sur l'organisation et le fonctionnement du Conseil National, modifiée, interdit désormais uniquement au Conseil National de faire ou de publier « *de proclamation à la population mettant en cause la Personne du Prince ou Ses fonctions* ».

Tenant compte de ces éléments, la Commission a, par délibération n° 2019-086 du 15 mai 2019, rendu un avis favorable à la mise en œuvre de ce traitement, tout en rappelant qu'il y a lieu de se conformer aux dispositions de l'article 80 bis de la Loi n° 839 sur les élections nationales et communales aux termes desquelles : « *Lorsqu'il est procédé à l'envoi de tout document, courrier, imprimé, bulletin d'information, message quels qu'en soient la forme et le support, ou à la réalisation d'enquêtes, les destinataires de ces envois et enquêtes sont informés de l'origine des informations ayant permis de les contacter, de l'identité de la personne pour le compte de laquelle la communication est réalisée et de leur possibilité de s'opposer, sans frais hormis ceux liés à la*

transmission de l'opposition, à l'utilisation de leurs informations nominatives ainsi que celle de se faire radier, sans frais, des traitements automatisés ou non d'informations nominatives qui ont été constitués à partir des renseignements contenus dans la liste électorale. »

LA SÉCURISATION DES NOUVEAUX LOCAUX DE LA CCIN PAR LE BIAIS DE CAMÉRAS, D'UN CONTRÔLE D'ACCÈS PAR BADGES MAGNÉTIQUES ET D'UNE ALARME

Suite à son déménagement au mois de juin 2019, la CCIN a souhaité mettre en place un dispositif de vidéosurveillance afin d'assurer la sécurité des biens et des personnes au sein de ses locaux sensibles ainsi qu'un système de contrôle d'accès par badges magnétiques et d'alarme, pour sécuriser les accès à ses locaux et limiter l'accès aux espaces comportant des données/équipements sensibles aux seuls agents habilités.

Ces dispositifs sont mis en place « *dans un but sécuritaire uniquement* ». C'est ainsi que les caméras n'ont été installées que dans les locaux comportant des documents/équipements sensibles, accessibles aux seuls collaborateurs habilités.

Par ailleurs, seuls le Secrétaire Général, en consultation en différé en cas d'incident, et le Service Technique qui a tous les droits dans le cadre des opérations de maintenance, y compris l'extraction, ont accès aux informations collectées.

Concernant le dispositif de contrôle d'accès, le prestataire pourra également avoir accès aux données dans le cadre de ses opérations de maintenance, mais cet accès se fera sous la supervision du Service Technique.

Les deux systèmes ont fait l'objet d'un avis favorable de la Commission en date du 20 novembre 2019, respectivement par la délibération n° 2019.171 et la délibération n° 2019-172.

LA MISE EN ŒUVRE D'UNE PLATEFORME DE E-SANTÉ

Afin de gérer un portefeuille de services numériques à destination des patients et des professionnels de santé autorisés à exercer en Principauté, le Gouvernement Princier a souhaité mettre en place un portail de e-Santé exploité par le Département des Affaires Sociales et de la Santé. Ce portail a été soumis à la Commission qui a émis un avis favorable par sa délibération n° 2019-169 du 20 novembre 2019.

Ce portail a pour fonctionnalités :

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

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

La Commission a pu constater que le traitement était entre autres justifié par le consentement des personnes concernées. En effet, le consentement des professionnels de santé est recueilli préalablement à la publication dans l'annuaire du portail des informations détaillées les concernant. En l'absence de consentement de leur part, seuls les éléments figurant sur leur autorisation d'exercer (nom, prénom, adresse, activité) sont publiés dans l'annuaire du portail, la Direction de l'Action Sanitaire ayant en effet pour mission de rendre publiques ces informations.

Les patients, quant à eux, doivent cocher la case d'acceptation des conditions générales d'utilisation du portail et avoir pris connaissance des informations relatives à la protection de leurs informations nominatives avant de valider la création de leur compte utilisateur.

La Commission a toutefois demandé que le traitement ayant pour finalité « G*estion des autorisations d'exercer des professionnels de santé* » lui soit soumis dans les plus brefs délais. Elle a également rappelé que les rapprochements et interconnexions avec les traitements liés à la gestion de prise de rendez-vous des établissements et praticiens libéraux doivent être effectués avec des traitements légalement mis en œuvre.

Enfin, la Commission a rappelé que les comptes utilisateurs devaient être protégés par un mot de passe réputé fort et que les comptes administrateurs devaient être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Elle a également pris acte du fait que les administrateurs systèmes n'avaient aucun accès aux données de santé des patients qui utiliseraient cette plateforme.

LA MISE EN PLACE D'UN OUTIL D'ORIENTATION POUR LES ÉLÈVES DE LA PRINCIPAUTÉ

La Direction de l'Education Nationale, de la Jeunesse et des Sports (DENJS) a soumis à la Commission une demande d'avis relative à une solution

dénommée « *CAESO* » qui, par le biais d'un algorithme, analyse certains aspects de la personnalité de l'élève pour lui proposer des métiers adaptés à celle-ci, en l'informant des filières et cursus qui semblent lui convenir. Cette analyse s'effectue par le biais de questions/réponses via un « *chatbot* » disponible sur la messagerie Messenger appartenant à Facebook.

La Commission a tout d'abord constaté que le traitement reposait notamment sur l'utilisation de réseaux sociaux américains, pays ne disposant pas au sens de la Loi n° 1.165 d'une législation d'un niveau adéquat en matière de protection des données personnelles, et dont l'utilisation relève d'un choix personnel des personnes concernées.

Aussi, elle a particulièrement veillé à ce que l'autorisation parentale soit la plus claire et exhaustive possible, et à ce que la durée de conservation soit maitrisée. Elle a également demandé que soit effectuée une sensibilisation des élèves à la vie privée en environnement numérique, concernant notamment la mise à disposition à des tiers de leur profil de personnalité via un URL ne requérant pas de mot de passe.

Afin de prendre en compte les éléments demandés par la Commission et son retour d'expérience, la DENJS est revenue auprès de la CCIN pour acter les évolutions de sa solution, qui ne passe plus désormais que par un site dédié hébergé dans un pays dont la législation en matière de protection des données personnelles est adéquate.

LES TRAITEMENTS EXPLOITÉS PAR LA DIRECTION DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION DE L'ETAT

En 2019, de nombreux traitements de la Direction des Réseaux et des Systèmes d'Information (DRSI) ont été soumis pour avis à la Commission.

La plupart de ces traitements concerne la gestion des informations nominatives dans le cadre du déploiement de la sécurité des systèmes d'information de l'Etat :

- « *Gestion du renouvellement des postes informatiques de l'Administration de l'Etat* » ;
- « *Gestion des habilitations et des accès au Système d'information* » ;
- « *Gestion des accès à distance au Système d'information du Gouvernement* » ;
- « *Sécurisation des accès à distance au SI pour les flottes nomades BYOD et professionnelles* ».

Ces traitements ont reçu un avis favorable de la Commission, qui a néanmoins pu constater que les outils déployés à des fins de sécurité collectaient souvent l'adresse IP des personnes concernées. Elle a pu distinguer deux cas. En ce qui concerne la collecte d'IP de personnes essayant de pénétrer les systèmes d'informations, leur nécessaire collecte s'analyse bien en une collecte d'informations nominatives indirectes. Toutefois, une information individuelle des personnes concernées n'est pas proportionnée. Par ailleurs, en ce qui concerne la collecte des adresses IP transmises par les terminaux BYOD des agents et fonctionnaires de l'Etat, la Commission a estimé qu'en l'absence de but sécuritaire, cette collecte devait être exclue.

Les autres traitements concernent les systèmes de messagerie du Gouvernement :

- « *Gestion de la messagerie électronique professionnelle Office 365* » ;
- « *Gestion de la messagerie électronique professionnelle Exchange* »

Concernant les traitements de messagerie, le responsable de traitement ayant indiqué que l'Agence Monégasque de Sécurité Nationale (AMSN) avait accès audit traitement, la Commission a tenu à rappeler ce qu'il fallait entendre par « *personne ayant accès au traitement* ». Aussi, l'AMSN n'avait-elle pas en l'occurrence un accès continu aux informations des messageries, mais disposait de prérogatives de sécurité encadrées par les dispositions de la Loi sur la criminalité technologique. La Commission a également rappelé à cette occasion que les traitements mis en œuvre par l'AMSN devaient lui être transmis pour avis.

Enfin, quelle que soit la nature des traitements concernés, la Commission a rappelé que l'information de toutes les catégories de personnes concernées devait être effectuée conformément à l'article 14 de la Loi n° 1.165.

LES TRAITEMENTS SOUMIS PAR LE SECRÉTARIAT GÉNÉRAL DU GOUVERNEMENT

Le Secrétariat Général du Gouvernement a désiré moderniser la préparation des Conseils de Gouvernement en adoptant une approche « *workflow* », c'est-à-dire un processus de validation par étapes, partant notamment de la création des délibérations par les Services de l'Administration jusqu'à l'adoption des décisions en Conseil.

Ce traitement s'inscrit dans le projet de dématérialisation des processus de l'Administration. Après avoir rappelé que les informations alimentant le traitement doivent avoir pour origine des traitements légalement mis en œuvre, la Commission a demandé que le traitement concerné ne serve pas de support à l'archivage à des fins historiques des documents objets du traitement, et a limité de ce fait à 5 ans en archive courante ou intermédiaire la durée de conservation des informations en son sein.

En outre, le Secrétariat Général de Gouvernement a également sollicité l'avis de la Commission relativement au traitement ayant pour finalité « *création, délivrance et suivi des passeports biométriques à puce et de documents de voyage* ». La Commission a d'une part rappelé certaines exigences de sécurité, notamment en termes d'accès aux informations et de chiffrement des extractions, et d'autre part encadré la collecte d'informations en provenance de la Mairie ainsi que leurs durées de conservation.

Ces deux traitements ont fait l'objet d'avis favorables de la Commission.

LA POURSUITE DU PROCESSUS DE DÉMATÉRIALISATION DES DÉMARCHES ADMINISTRATIVES

En 2019, trois demandes d'avis ont été déposées par l'Administration concernant la mise en œuvre des traitements permettant notamment de simplifier et de dématérialiser les démarches administratives.

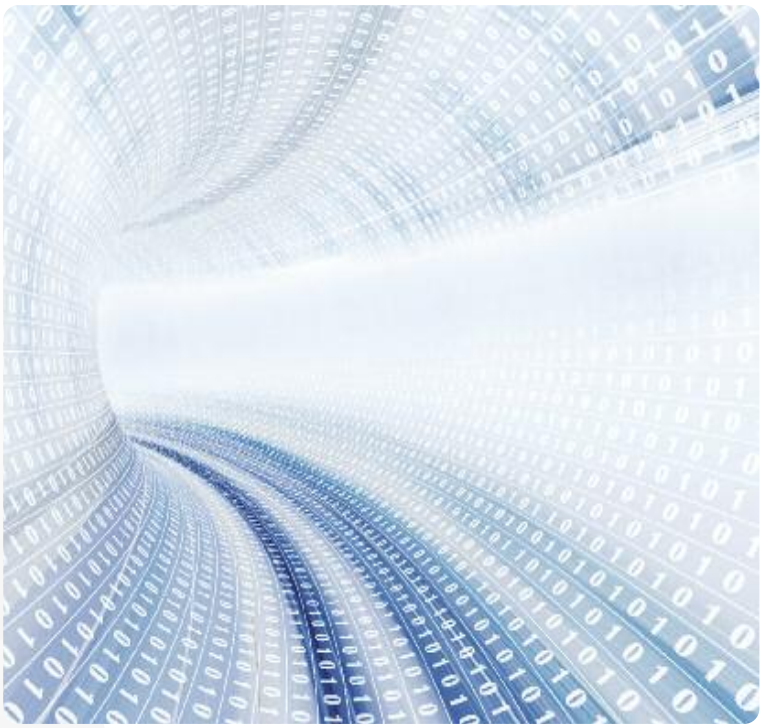
L'accueil des stagiaires en entreprise mis en œuvre par la Direction du Travail

Premièrement, la Direction du Travail – Service de l'emploi a sollicité l'avis de la Commission concernant le traitement dont la finalité est « *Déclarer l'accueil de stagiaire en entreprise* ».

Il concerne les entreprises monégasques accueillant des stagiaires au sein de leur structure qui ont l'obligation de communiquer au Service de

l'emploi les informations relatives aux conventions de stage, afin de vérifier notamment qu'il ne s'agit pas d'un stage devant faire l'objet d'une procédure de demande d'autorisation d'embauche. Afin de faciliter cette démarche, la Direction du Travail a souhaité mettre en œuvre un télé-service permettant aux entreprises de facilement informer le Service de l'emploi de l'accueil d'un stagiaire.

Ce traitement a fait l'objet d'avis favorable de la part de la Commission. Cependant, elle a rappelé que la justification du traitement par le consentement, formalisé par l'obligation d'accepter les conditions générales d'utilisation au moment de la création du compte, ne vaut que pour les personnes auprès de qui la Direction du Travail collecte directement l'information, à savoir les personnels des entreprises monégasques accueillant des stagiaires et effectuant les démarches en ligne. Aussi, la Commission a demandé que les stagiaires soient également informés de manière conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993. Il appartient ainsi aux entreprises monégasques accueillant des stagiaires de les informer de la collecte et du traitement de leurs données.



La Direction des Ressources Humaines et de la Formation de la Fonction Publique pour les candidatures spontanées

Par ailleurs la Direction des Ressources Humaines et de la Formation de la Fonction Publique (DRHFFP) a déposé une demande d'avis concernant le traitement dont la finalité est « *Déposer une candidature spontanée aux emplois de l'Administration Monégasque* ».

Afin de faciliter les démarches des administrés cherchant un emploi et de permettre à la DRHFFP de gérer un catalogue de CVs, l'Etat a souhaité mettre en œuvre un télé-service permettant un dépôt sécurisé des candidatures spontanées.

Le traitement a reçu un avis favorable de la Commission qui a néanmoins rappelé qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. De plus en cas de collecte d'une copie d'un document d'identité, sa transmission et son traitement devront faire l'objet de mesures de protection particulières. La durée de conservation des informations relatives aux candidats a été ramenée à 2 ans, par la Commission, considérant qu'une durée de 5 ans n'était pas pertinente en l'espèce.

Le traitement a reçu un avis favorable de la Commission qui a demandé que la politique de mot de passe soit renforcée, que les identifiants soient supprimés dès que l'utilisateur n'est plus habilité à accéder au traitement et que les logs des utilisateurs soient conservés au minimum 3 mois et au maximum un an.

Pour les trois traitements sus-évoqués, la Commission a également rappelé certaines exigences de sécurité.

La gestion des autorisations administratives par la Direction de l'Aménagement Urbain

La Direction de l'Aménagement Urbain (DAU) a soumis à la Commission une demande d'avis relative au traitement dont la finalité est « *Gestion informatique des autorisations administratives délivrées par la Direction de l'Aménagement Urbain* ».

La DAU a en effet souhaité rationaliser la gestion des demandes d'autorisations qu'elle traite. A cette fin, elle a souhaité mettre en œuvre un progiciel dénommé LITTERALIS dans lequel seront exploitées des informations nominatives.

LA MISE EN PLACE D'UN PORTAIL INTRANET POUR LES SERVICES DE L'ETAT

Le Ministre d'Etat a sollicité l'avis de la Commission concernant le traitement dont la finalité est « *Mettre en place un portail intranet de services pour les employés du Gouvernement de Monaco munis d'un poste de travail* » visant à déployer au sein de l'Administration un Intranet doté d'outils collaboratifs permettant de « *centraliser les ressources nécessaires aux agents et fonctionnaires (liens, documents, etc.)* ». Le traitement a été justifié par l'intérêt légitime de la transformation digitale de l'Administration et a reçu un avis favorable de la Commission. Cependant elle a rappelé certaines exigences concernant l'exercice du droit d'accès par voie électronique, notamment concernant la vérification de l'identité du demandeur. De plus, elle a rappelé certaines exigences de sécurité ainsi que le fait que l'ensemble des personnes concernées devait faire l'objet d'une information préalable conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Enfin, la Commission a encadré la durée de conservation des informations figurant sur le profil de l'agent ou fonctionnaire en la portant de 5 ans à 3 mois maximum après son départ de l'Administration. En ce qui concerne les données d'horodatage et de connexion, la durée de leur conservation a été fixée à 1 an.

UN RÉSEAU SOCIAL INTERNE À L'ADMINISTRATION

La Direction des Ressources Humaines et de la Formation de la Fonction Publique (DRHFFP) a soumis à la Commission une demande d'avis relative au traitement dont la finalité est « *Gestion du réseau social de l'Administration monégasque : Workplace* ».

La DRHFFP a désiré moderniser les relations de travail en mettant à disposition des personnels de l'Administration un espace dédié à la diffusion d'informations et permettant la constitution de groupes transversaux entre les différents services et départements.

A l'analyse du dossier, la Commission a relevé que le traitement s'appuyait sur une architecture Facebook et que le prestataire installait des cookies pour son propre compte dont certains ne servent pas uniquement au fonctionnement du site mais à l'amélioration des services/performances, ou encore à l'édition de statistiques, notamment par le biais de Google Analytics, ce qui induit un transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat en matière de protection des informations nominatives.

En conséquence, la Commission a émis un avis défavorable à la mise en œuvre de ce traitement et a demandé au responsable de traitement qu'avant toute mise en service de Workplace les utilisateurs soient préalablement informés que des cookies sont déposés dans leurs terminaux par le prestataire de service et qu'ils soient en mesure de paramétrer leur dépôt.

De plus le responsable de traitement doit vérifier d'une part l'existence de transferts des informations nominatives, effectués par certains cookies déposés, vers un/des pays ne disposant d'un niveau de protection adéquat en matière de protection des informations nominatives et d'autre part l'accès des administrateurs Facebook sis aux USA aux informations nominatives, et le cas échéant effectuer les formalités relatives aux transferts indiquant toutes les mesures prises conduisant au respect des droits des personnes concernées.

Enfin, le responsable de traitement doit également s'assurer qu'aucun des administrateurs/modérateurs n'ait accès au chat privé, eu égard au secret des correspondances.

Concernant la durée de conservation, elle a rappelé que l'archivage de 5 ans ne devrait pas être réalisé.

L'OUTIL DE SIGNALEMENT DES NUISANCES URBAINES

La Direction du Développement des Usages Numériques (DDUN) a soumis à la Commission une demande d'avis relative au traitement dont la finalité est « *Mise à disposition des usagers d'une application permettant le signalement de nuisances urbaines pour transmission aux Directions de l'Administration concernées* » dénommé « *Urban Report* ».

Par ce traitement la DDUN a souhaité mettre à disposition des administrés une application permettant de recueillir des signalements urbains, tels que du « *mobilier urbain détérioré, nuisances de chantier, signalement de méduses, remontée positive/compliment sur jardin ou massif floral...* ».

L'intérêt de cette solution est également de permettre « *aux services métiers d'organiser, de traiter et de piloter le suivi des actions (prise en charge du traitement des signalements effectués par les usagers de l'application mobile, supervision des contrôles chantiers, liés ou pas aux signalements des usagers* ».

Ce traitement a fait l'objet d'un avis favorable de la part de la Commission qui a néanmoins demandé, au regard de la nature particulière du traitement, que les mentions d'information délivrées aux usagers les enjoignent expressément à ne pas communiquer d'informations nominatives relatives à des tiers afin d'éviter que l'outil ne puisse être utilisé en tant qu'outil de délation.

En outre, la Commission a d'une part rappelé que les personnels de l'Administration doivent également être informés de leurs droits, et a d'autre part fixé la durée de conservation des signalements au temps de leur résolution.

LA VIDÉOSURVEILLANCE DES LOCAUX DE LA RÉGIE MONÉGASQUE DES TABACS ET ALLUMETTES

« *Etant exposée à un risque de cambriolages et d'agressions lié à la nature des marchandises entreposées* », la Régie Monégasque des Tabacs et Allumettes a souhaité se doter d'un dispositif de vidéosurveillance qui a fait l'objet d'un avis favorable de la Commission par délibération n° 2019-074 du 15 mai 2019.

Après avoir constaté qu'aucun accès distant n'est utilisé sur le réseau de vidéosurveillance et rappelé entre autres que la réponse à un droit d'accès doit s'exercer uniquement sur place, la Commission a précisé que toute copie ou extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

LE RÈGLEMENT DES FOURNISSEURS PAR LA SOCIÉTÉ MONÉGASQUE DES EAUX

Dans le cadre de ses activités, la Société Monégasque des Eaux (SMEaux) se doit de traiter dans les plus brefs délais, par le biais de son logiciel comptable de paiement, le nombre important de factures qu'elle reçoit.

A cet effet, elle a obtenu un avis favorable de la Commission par délibération n° 2019-113 en date du 17 juillet 2019 à la mise en œuvre d'un traitement automatisé ayant pour fonctionnalités :

- « *l'enregistrement comptable des factures, conformément aux bons de livraison dans la base comptable informatique dénommée « LD Compta » ;*
- *le règlement des fournisseurs, par lettre chèque, effectué par le même logiciel et sur la même base* ».

La SMEaux demande ainsi divers renseignements (nom, adresse, code postal et ville, entre autre, du fournisseur), uniquement à des fins de règlement, qui sont stockés dans le logiciel comptable permettant aux utilisateurs de ce dernier (le comptable et le responsable administratif) de régler les fournisseurs par l'émission de lettres chèques.

Après avoir rappelé notamment que toutes les personnes concernées devaient faire l'objet d'une information préalable, la Commission a considéré qu'une procédure relative au droit d'accès par voie électronique devait 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.

Elle a par ailleurs considéré que les experts comptables de la société pouvaient également être destinataires des informations objet du traitement.

Enfin, la Commission a demandé que le traitement ayant pour finalité « *Gestion de la sécurité des accès utilisateurs* » lui soit soumis dans les plus brefs délais.

LE DÉVELOPPEMENT DE NOUVEAUX SERVICES PAR MONACO TELECOM

En 2019, Monaco Telecom a sollicité la CCIN relativement à trois dossiers qui ont reçu un avis favorable.

Le premier d'entre eux concerne le déploiement en Principauté de deux services regroupés sous la finalité « *Gestion des services Monaco Care Safety et Monaco Care password.* » Le premier concerne une protection multi-équipements contre les menaces de l'Internet tandis que le second permet la gestion de mots de passe multi-équipements, le

tout ayant pour objectif d'améliorer la sécurité des terminaux en Principauté.

Le second traitement concerne la mise à disposition des clients d'une application de suivi de consommation de services en lien avec les contrats qu'ils ont souscrits.

Il appartient ainsi aux personnes désireuses de la télécharger et d'en accepter les conditions générales d'utilisation, « *qui détaillent l'utilisation faite des données et que l'utilisateur doit accepter avant de pouvoir utiliser l'application* ».

Enfin, la Commission a été saisie d'une demande d'avis concernant la « *Gestion du service de télévision sur IP* » afin que Monaco Telecom puisse proposer à ses clients ayant un abonnement internet résidentiel un service de télévision par IP permettant de visualiser des chaînes de télévisions sur leurs différents terminaux. La Commission a demandé que l'information des personnes concernées soit conforme aux dispositions de l'article 14 de la Loi n° 1.165.

LES TRAITEMENTS DU CHPG

Le Centre Hospitalier Princesse Grace a poursuivi en 2019 sa mise en conformité avec la Loi n° 1.165 du 23 décembre 1993 avec le dépôt de cinq nouvelles demandes d'avis.

Par délibération n° 2019-021 du 20 février 2019, la Commission a ainsi émis un avis favorable à la mise en œuvre du traitement ayant pour finalité « *Gestion de l'adressage IP* » qui permet à l'hôpital de suivre les adressages IP des ressources connectées à son réseau et d'effectuer un inventaire physique desdites ressources.

Le même jour, la Commission s'est également prononcée favorablement sur le traitement ayant pour finalité « *Gestion du hotspot public du CHPG* » après avoir relevé que les patients, les visiteurs et les professionnels de santé disposent d'un accès à internet via le hotspot gratuit de l'hôpital qui ne peut être ouvert qu'après l'acceptation expresse des conditions générales d'utilisation.

Le 20 mars, la Commission a émis un avis favorable à la mise en place par le CHPG d'un système anti-fugue destiné à assurer la protection des patients du Centre Rainier III présentant des troubles cognitifs. Dans le cadre de ce traitement, seuls les logs de connexion, l'historique des alarmes et les informations liées au médaillon (numéro de tag, numéro de chambre et référence de porte) sont collectés. L'information préalable des personnes concernées est effectuée par le biais d'un document spécifique. La Commission a cependant demandé que cette information préalable soit également effectuée auprès des représentants des patients concernés si ceux-ci ne sont pas en capacité de recevoir cette information.

Le traitement ayant pour finalité « *Gestion de la communication interne* » qui permet à l'hôpital de diffuser des informations par le biais de l'Intranet a lui-aussi fait l'objet d'un avis favorable le 18 septembre 2019 par délibération n° 2019.128. Après avoir rappelé que l'information des salariés devait impérativement être conforme aux dispositions de l'article 14 de la Loi n°1.165 du 23 décembre 1993, la Commission a considéré que les communications qui revêtent un caractère nominatif ne devaient être conservées que pour la durée pendant laquelle elles sont pertinentes.

Enfin, elle a émis un avis favorable le 31 octobre à la gestion du « *Plan blanc* » qui est déclenché par le Directeur du CHPG ou son représentant, à l'initiative du Chef de Service des Urgences ou de son représentant, dès lors que le CHPG se trouve confronté à la prise en charge simultanée de six victimes graves. Elle a cependant demandé que la communication par voie électronique de la liste des personnes à ajouter ou à retirer du plan blanc ainsi que la connexion en interne au logiciel d'appel groupé soient toutes deux sécurisées.

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

En 2019 la Commission a émis 7 avis favorables à la mise en œuvre de recherches médicales, 5 pour des études biomédicales et 2 pour des études non-biomédicales, toutes présentées par le Centre Hospitalier Princesse Grace (CHPG).

Les recherches biomédicales

Par deux délibérations en date du 23 janvier 2019, la Commission a ainsi émis un avis favorable à deux recherches menées par le Centre Antoine Lacassagne, situé à Nice et représenté en Principauté par le CHPG.

La première, dénommée « *Etude ICAR* », devrait concerner environ 4 patients suivis par le Service radiothérapie du CHPG. Elle a pour objectif principal de déterminer la Dose Maximale Tolérée (DMT) et la Dose Recommandée (DR) de l'acétazolamide en association avec la radiothérapie combinée à une chimiothérapie à base de sels de platine et d'étoposide.

La deuxième étude est dénommée « *Etude FDG-IMMUN* » et a pour objectif principal de déterminer, dès la première progression métabolique observée en TEP au 18FDG, un seuil de l'index de rétention du 18FDG (mesuré par une acquisition dual-point) permettant de distinguer une vraie progression tumorale d'une pseudo-progression d'origine inflammatoire infiltrat leucocytaire. Elle devrait concerner une dizaine de patients à Monaco suivis au sein de l'Hôpital de Jour.

Pour ces deux recherches, la Commission a relevé que la note d'information indique que le patient a le droit de retirer son consentement et de s'opposer à tout moment au traitement de ses données. Cette note prévoit en outre qu'en cas de retrait du consentement ou d'opposition au traitement de ses données, le patient pourra « *demander l'effacement de celles déjà collectées lorsque celles-ci ne sont plus nécessaires ou s'il n'existe aucune autre exigence légale qui requiert leur utilisation (par exemple, l'évaluation du médicament à l'étude par les autorités compétentes, le promoteur ou pour s'assurer* » que les intérêts légitimes du patient ne seront pas compromis).

La Commission a en revanche constaté que le formulaire de consentement ne mentionnait pas l'existence de ce droit pour le patient ainsi que les éventuelles conditions requises pour cet effacement. Elle a donc demandé que ledit document soit modifié en ce sens.

Le 18 septembre 2019, la Commission a émis un avis favorable à la mise en place par VIFOR France, représenté en Principauté de Monaco par le CHPG, d'une recherche biomédicale dénommée « *Etudes CARENFER* » destinée à étudier la prévalence de la carence martiale chez des patients présentant soit une insuffisance cardiaque (CARENFER IC), soit atteints d'un cancer (CARENFER ONCO-HEMATO). A cet égard la Commission a tenu à préciser que si l'état des patients ne leur permettait pas de consentir de manière libre et éclairée à la participation à cette étude, il incombait au responsable de traitement de recueillir le consentement de leurs représentants dûment habilités.

En outre, après avoir relevé que la lettre d'information prévoyait qu'en cas de retrait du consentement ou d'opposition au traitement de ses données, le patient pouvait signaler au médecin investigateur qu'il ne souhaitait pas que les données collectées soient utilisées mais que le promoteur à qui ce souhait aura été transmis « *pouvait ne pas faire droit à cette demande afin de ne pas compromettre gravement la réalisation des objectifs de la recherche* », la Commission a toutefois noté que le formulaire de consentement ne comportait aucune mention sur ce point.

Elle a en conséquence demandé que ledit document soit modifié afin de préciser qu'en cas de retrait du consentement le promoteur pouvait ne pas faire droit à cette demande afin de ne pas compromettre gravement la réalisation des objectifs de la recherche.

Enfin, concernant le sous-traitant du prestataire en charge du Data Management, la Commission a demandé au responsable de traitement de s'assurer que ledit sous-traitant était bien soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au prestataire.

La Commission a également émis un avis favorable à la mise en œuvre de l'étude dénommé « *CAPUERA* » dont le promoteur est le Centre Hospitalier Universitaire de Nice. Ladite étude a pour objectif principal de déterminer l'impact diagnostic de l'échographie pleuro-pulmonaire comparativement à la radiographie de thorax dans la prise en charge d'une suspicion clinique de pneumopathie aiguë communautaire (PAC) sans signe de gravité chez un patient consultant aux urgences.

La Commission a cependant demandé que le « *consentement éclairé* » soit modifié afin d'indiquer que les données recueillies avant l'opposition d'un patient pourront être conservées et traitées dans les conditions prévues par la recherche et que la « *Notice d'information* » soit modifiée afin d'indiquer que les données sont uniquement identifiées par un numéro d'identification.

Enfin, par une délibération en date du 18 décembre 2019, la Commission s'est prononcée sur une recherche présentée par le Centre Hospitalier Universitaire (CHU) de Nice, dénommée « *Etude SPOT* ». Cette recherche monocentrique qui a pour objectif principal de démontrer que l'administration de L-tyrosine a un effet protecteur sur l'anxiété péri-opératoire devrait concerner au total 100 patients pris en charge pour une cure de hernie inguinale unilatérale ou bilatérale sous anesthésie générale en ambulatoire.

Si elle a émis un avis favorable à la mise en œuvre de cette recherche, la Commission a toutefois relevé que le responsable de traitement indiquait qu'en cas de retrait de consentement à la participation à la recherche, les données du participant pourront être supprimées mais que les deux documents d'information étaient silencieux sur ce point.

Elle a donc demandé que lesdits documents soient modifiés afin d'indiquer qu'en cas de retrait de l'étude, le patient pourra demander que les données déjà collectées soient supprimées.

En outre, la Commission a noté que la « *Notice d'information* » indiquait que lesdites données

seraient identifiées par un numéro de code ainsi que par la première lettre du nom et la première lettre du prénom du patient, alors que celui-ci est en réalité identifié par un « *numéro de patient* » attribué par le médecin investigateur par ordre d'inclusion. Elle a ainsi demandé que ladite notice soit modifiée en conséquence.

Parallèlement à ces 5 études biomédicales, la Commission a eu à se prononcer sur 2 recherches non biomédicales.

Les recherches non biomédicales

Elle a ainsi émis le 15 mai 2019 un avis favorable à la mise en place d'un traitement automatisé de données au sein du Département de Gérontologie Clinique Rainier III du CHPG dans le cadre d'une étude observationnelle menée par l'hôpital E.O. Galliera Hospital, localisé à Gênes, en Italie.

Dénommée « *EUROSAF* », cette recherche a pour objectif principal d'évaluer, dans une population de sujets âgés hospitalisés atteints de fibrillation auriculaire, le rapport bénéfice/risque des traitements anticoagulants en termes de mortalité (toutes causes confondues), d'évènements thromboemboliques (accidents vasculaires cérébraux, embolie systémique) et d'hémorragies (notamment saignements intracrâniens et gastro-intestinaux).

Après avoir constaté que le formulaire d'information indiquait que le dossier médical ne pourra être consulté que sous la responsabilité du médecin qui suit le patient dans le cadre de cette *étude et qu'il « ne pourra être accessible qu'aux personnes mandatées par le Promoteur de la recherche, ainsi qu'aux Autorités de Santé, dans le plus strict respect du secret professionnel* », la Commission a demandé qu'il soit précisé dans ledit formulaire que le dossier médical du patient et les informations directement nominatives le concernant ne pourront être consultables qu'au CHPG.

Elle a en outre demandé que le consentement que signe le patient soit complété afin que ledit patient

soit informé que s'il désire arrêter sa participation à l'étude, il pourra signaler au médecin investigateur qu'il ne souhaite pas que les données recueillies soient utilisées et que ledit médecin investigateur en avertira le promoteur mais que ce dernier pourra cependant « *ne pas faire droit à cette demande afin de ne pas compromettre gravement la réalisation des objectifs de la recherche* ».

Enfin, par délibération en date du 17 juillet, l'étude non interventionnelle dénommée « *Registre SVV-SAS* » mise en œuvre par le Pôle d'Exploration des Apnées du Sommeil (PEAS) a reçu un avis favorable de la Commission. Menée au sein du service de cardiologie du CHPG, cette recherche pour objectif principal de démontrer que la restauration de la continuité du sommeil par la pression position continue (PPC) ou l'orthèse d'avancée mandibulaire (OAM) (chez les patients intolérants), entraîne une diminution rapide et significative du nombre des syncopes, voire leur disparition.

La Commission a cependant tenu à rappeler que le dossier médical du patient et les informations directement nominatives le concernant ne pourront être consultables qu'au CHPG. Elle a également demandé que les identifiants et mots de passe du personnel habilité du CHPG soient individuels.

7

LES AVIS DE LA COMMISSION SUR LES PROJETS DE TEXTES LEGISLATIFS ET REGLEMENTAIRES

Formalisant la volonté forte de faire prendre à la Principauté un « v*irage numérique* » le Gouvernement a saisi la Commission de deux projets de Loi portant respectivement sur l'identité numérique et sur l'économie numérique.

PROJET DE LOI RELATIVE À L'IDENTITÉ NUMÉRIQUE

Par délibération n° 2019-120 du 18 septembre 2019, la Commission a rendu son avis sur ce projet de Loi qui a vocation à instaurer une citoyenneté numérique au moyen de processus fiables qui permettent l'identification et l'authentification des personnes dans l'environnement numérique.

Si la Commission a bien perçu l'importance des enjeux résultant de ce projet, elle a regretté que, dans la version dont elle a été saisie, le dispositif projeté ne comportait que 10 articles, les nombreux renvois à des textes réglementaires d'application, dont elle n'a pas eu connaissance, empêchant la bonne compréhension des mesures envisagées.

Dans sa délibération portant avis sur ce projet de Loi elle a ainsi souligné l'impossibilité de déterminer avec certitude à qui pouvait être attribué une identité ou un identifiant numérique, et de ce fait les difficultés qui en découlent concernant le processus d'authentification. Les imprécisions de rédaction créant des difficultés de compréhension concernant l'attribution de l'identifiant numérique, la Commission a relevé que, même si le projet de Loi constituait une « *Loi cadre* », il importait toutefois que ce socle législatif soit suffisamment clair et précis eu regard des conséquences en découlant pour les personnes concernées.

Sur ce point elle s'est plus particulièrement interrogée sur la place du consentement des personnes concernées qui pourrait, ou devrait, être introduit en fonction des différents cas d'authentification envisagés, rappelant ainsi les différents choix d'attribution d'identité numérique effectués par les pays cités dans l'exposé des motifs du texte soumis.

Le quantum des informations collectées au titre de l'identité numérique a de plus conduit la Commission à relever que, si les articles en projet ne le déterminaient pas, le troisième alinéa de l'article 2 précisait que « *l'identification des personnes physiques est établie notamment sur la base de données biométriques transformées en une empreinte numérique* ». Aussi elle a rappelé la sensibilité de ce type de données, et le fait que leur collecte devait être prévue de manière précise, dans les stricts cas où la finalité de leur traitement pourrait le justifier.

Les dispositions relatives au « *registre national monégasque* » ont également suscité des observations de la part de la Commission, s'agissant notamment :

- de son futur rôle dans la création de documents d'identité ;
- de l'identification de la / des Autorité(s) dont dépendra la tenue de ce registre ;
- de son contenu précis ;
- de son alimentation, et des durées de conservation des informations qu'il contiendra (notamment de traçabilité des accès) ;
- des modalités de consultation des informations qu'il contiendra.

L'émergence de la notion de « *citoyenneté numérique* », prolongement immédiat d'une approche qui place le numérique autour de l'individu, étant étroitement liée aux droits fondamentaux des personnes concernés, la Commission a estimé qu'une responsabilisation du porteur de l'identité numérique, se devant de la protéger, devrait être insérée aux dispositions du projet.

De plus, la saisine concomitante sur le projet de Loi sur l'économie numérique, devenu dans sa version promulguée la Loi pour une Principauté numérique, a conduit la Commission à noter que certaines des définitions projetées dans les deux projets étaient différentes. Si elle a entendu les explications des Services de l'Etat selon lesquelles chaque définition n'avait de valeur juridique qu'en égard au texte dans lequel elle était inscrite, elle s'est cependant inquiétée de l'incompréhension et de l'insécurité juridique que cette dichotomie pourrait inévitablement créer.

PROJET DE LOI RELATIVE À L'ÉCONOMIE NUMÉRIQUE : LOI POUR UNE PRINCIPAUTÉ NUMÉRIQUE

Saisie par le Ministre d'Etat le 28 mars 2019 d'un projet de Loi sur l'économie numérique, renommée « *Loi pour une Principauté numérique* », la Commission a émis un avis par délibération n° 2019-121 en date du 18 septembre 2019.

Ce projet de Loi met en exergue les principes de neutralité des réseaux, de loyauté des plateformes de services numériques et de sécurité juridique et technique des échanges numériques. Avec le Cloud et l'identité numérique, cette Loi représente la base du modèle monégasque dans un monde numérique.

Si elle a constaté que les dispositions envisagées par le projet de Loi étaient en grande partie similaires à celles contenues au sein du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit « *Règlement eIDAS* », la Commission a rappelé que ce règlement a pour objet de sécuriser les interactions dans un environnement électronique afin d'instaurer « *un climat de confiance (...) essentiel au développement économique et social* ».

A cet égard, elle a relevé l'absence de définition du service de confiance qualifié, présente dans le Règlement eIDAS et dans la définition du prestataire de service de confiance qualifié. Or, l'objectif est de renforcer la confiance dans le numérique en instaurant des standards de sécurité pour les services de confiance qualifiés.

Elle n'a pas manqué de relever que l'Ordonnance n° 3.413 du 2 aout 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré contient en son Titre IV « *De l'administration électronique* » des dispositions intéressant le numérique. Est notamment érigé aux termes des articles 45 et 54 de cette Ordonnance un référentiel général de sécurité destiné à définir les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage des téléservices, dont l'accusé de réception électronique, ainsi que l'opposabilité des démarches opérées par les administrés par voie électronique.

Aussi, la Commission s'est interrogée sur la pérennité des mesures mises en place par l'Administration et sur le fait de savoir si celle-ci sera enjointe d'appliquer les règles génériques des services de confiance prévues par le projet dont s'agit ou si elle continuera à fonctionner selon les règles de sécurité propres à l'Ordonnance

n° 3.413. Cela se pose particulièrement pour les dispositions de l'article 34 projeté qui infère sur les relations électroniques entre l'Administration et les administrés, mais également pour les dispositions de l'article 4 du projet de Loi sur l'identité numérique qui renvoie au référentiel AMSN pour la sécurité des identifiants numériques délivrés par la Principauté.

Concernant la territorialité du dispositif, la Commission a souligné que les services de confiance ne disposent de cette reconnaissance qu'en ce qui concerne le territoire de la Principauté, plus encore pour l'archivage électronique qui n'est pas un service de confiance au sens du règlement eIDAS et qui ne peut l'être qu'au niveau des législations nationales.

Monaco ne faisant pas partie de l'Union européenne, les standards que la Principauté établira ne vaudront que pour son territoire. Aussi, la Commission a fait part de l'intérêt qu'il y aurait à intégrer des mécanismes de reconnaissances mutuelles entre Etats dans le dispositif en projet, et ce afin de renforcer la sécurité et la confiance en la matière.

Elle s'est par ailleurs interrogée sur la parfaite articulation entre les domaines couverts par le coffre-fort numérique, les dispositions de l'article 16 relatif à la copie fiable et de sa future Ordonnance Souveraine d'application, et les dispositions de l'article 33 qui introduit les effets juridiques de l'archivage électronique et consacre sa valeur probante, l'objectif premier de ses observations étant d'assurer à la future législation interne un caractère suffisamment précis et prévisible pour en faciliter la compréhension et donc l'application.

Concernant le coffre-fort numérique la Commission a appelé de ses vœux l'intégration de garanties en termes d'intégrité, de disponibilité, de confidentialité des données stockées et de mise en œuvre des mesures de sécurité adéquates, afin de parachever le dispositif projeté.

Les articles 34 à 38 du projet de Loi tel que transmis à la Commission ont vocation à régir les échanges électroniques dans le cadre de procédures administratives. Comme elle l'a fait au titre du projet de Loi relatif à l'identité numérique, la Commission s'est inquiétée de l'imbrication des dispositions projetées avec l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré. Ainsi l'article 36 projeté fait référence directement à la notion de téléservice, qui n'est pas définie dans le projet de Loi mais dans l'Ordonnance Souveraine susvisée. Eu égard aux ambitions du projet Loi et de l'aspect parfois lacunaire de l'Ordonnance Souveraine dans l'encadrement des téléservices, la Commission a recommandé de les définir plus largement au sein du présent projet de Loi. Cela afin notamment de permettre à la Commission, qui n'avait pas été saisie à l'époque, de se prononcer sur les dispositions de l'Ordonnance Souveraine qui comportent des problématiques de protection de données personnelles importantes, mais également de faire mention dans le présent projet des mesures de sécurité devant être employées pour ce type de relation entre les usagers et les organismes du secteur public.

S'agissant plus spécifiquement du projet d'article 35 du projet de Loi, la Commission a noté que dans le cadre de leurs missions, les organismes du

secteur public pouvaient échanger entre eux des informations ou données des usagers déjà en leur possession et strictement nécessaires au traitement des demandes et déclarations soumises par ce même usager. Cet échange d'informations et de données de l'usager est préalablement soumis au consentement de celui-ci et doit s'effectuer dans « *le respect des dispositions en vigueur relatives à la protection des données à caractère personnel* ». Conformément à l'alinéa 2 de l'article 35, ce consentement se fonde sur l'information de l'usager qui doit connaître « *les informations ou données qui sont nécessaires à l'instruction de sa demande ou au traitement de sa déclaration et celles qu'il se procure directement auprès d'autres organismes du secteur public dont elles émanent* ». Aussi, la Commission a rappelé que le consentement vaut pour une finalité spécifique, ce qui suppose qu'il soit redonné par la personne concernée pour toute nouvelle démarche. Elle a de plus souligné que certaines Autorités publiques, telles que la Direction de la Sûreté Publique, devraient être écartées de ce dispositif, soit en listant les organismes éligibles, soit en listant ceux qui ne peuvent bénéficier de cette facilité.

En outre, la Commission a une nouvelle fois relevé l'existence de nombreux renvois à des Ordonnances Souveraines ou des Arrêtés Ministériels d'application, ce qui dilue la prévisibilité pour la Commission des mesures projetées et rend son appréhension encore plus technique pour les administrés.

La Commission a constaté que les Loi n° 1.482 pour une Principauté numérique et n° 1.483 relative à l'identité numérique, du 17 décembre 2019, ont été enrichies très substantiellement par rapport aux projets initiaux qui lui avaient été soumis.

PROJET D'ORDONNANCE SOUVERAINE RELATIVE AUX DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL PRODUITES OU REÇUES PAR LES PROFESSIONNELS ET ÉTABLISSEMENTS DE SANTÉ

Par sa délibération n° 2019-122 en date du 18 septembre 2019, la Commission a émis un avis sur la consultation du Ministre d'Etat relative au projet d'Ordonnance Souveraine relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé.

Après avoir relevé que certaines notions méritaient d'être précisées, notamment celle relative aux données de santé et à la durée de conservation du dossier médical, et que les modalités d'information préalable des personnes concernées devaient être définies, la Commission s'est attachée à rappeler les mesures de sécurité à prendre pour assurer l'intégrité et la confidentialité des informations collectées qui sont, en raison de leur nature, particulièrement sensibles.

C'est ainsi qu'elle a par exemple souligné l'importance d'un chiffrement fort des données de santé et la nécessité de mettre en place une politique d'authentification forte pour tout accès au dossier médical en ligne. A cet égard, la Commission a recommandé que des niveaux d'habilitation différenciés soient créés en fonction des missions des différentes personnes pouvant avoir accès aux informations et que cette politique d'habilitation soit tenue à jour et revue régulièrement.

Elle a par ailleurs tenu à mentionner que tout accès au dossier médical devait être impérativement journalisé afin de permettre la traçabilité des accès et l'historique des connexions.

Si la Commission s'est par ailleurs félicitée des dispositions de l'article 2 alinéa 2 du projet de texte imposant l'avis de la CCIN comme prérequis obligatoire avant que le référentiel d'interopérabilité et de sécurité établi par le Directeur de l'Agence Monégasque de Sécurité Numérique (AMSN) puisse être approuvé par Arrêté Ministériel, elle a toutefois regretté l'absence d'information de la CCIN en cas d'incident grave de sécurité des systèmes d'information.

La Commission a en effet estimé qu'en tant qu'Autorité en charge de la protection des données personnelles en Principauté elle devait être informée de tout incident affectant les données de santé à caractère personnel, d'autant plus que cette obligation d'information de la CCIN a été introduite pour la première fois en Principauté en matière d'échanges d'informations à des fins fiscales, et devrait donc tout naturellement être prévue lorsque les informations concernées sont des données aussi sensibles que les données de santé.

LE PROJET D'ARRÊTÉ MINISTÉRIEL FIXANT LES BONNES PRATIQUES TRANSFUSIONNELLES

Le 5 novembre 2018, le Ministre d'Etat a saisi la Commission dans le cadre de l'élaboration d'un projet d'Arrêté Ministériel destiné à fixer les principes de bonnes pratiques transfusionnelles en Principauté.

Inspiré par les dispositions françaises, ce nouveau texte abroge l'Arrêté Ministériel n° 2015-68 du 2 février 2015 fixant les principes de bonnes pratiques transfusionnelles afin de « *permettre une meilleure lisibilité* » dudit texte et assurer ainsi la plus grande sécurité de la chaîne transfusionnelle.

Dans le cadre de sa saisine la Commission s'est attachée à l'examen de la ligne directrice relative aux systèmes d'information, et aux dispositions en lien avec lesdits systèmes d'information, pour formuler des observations qui, pour la plupart, ont

été reprises dans la version finale de l'Arrêté Ministériel n° 2019-328 du 12 avril 2019.

C'est ainsi que concernant la ligne directrice, le terme de « *plans de maintenance* » a été complété conformément à la remarque de la Commission afin de préciser que ces plans comprennent les activités, les procédures, les ressources et la durée nécessaire pour exécuter la maintenance.

Par ailleurs, la sécurité du mot de passe permettant au personnel de s'authentifier a été renforcée en indiquant que ce mot de passe devait être réputé fort.

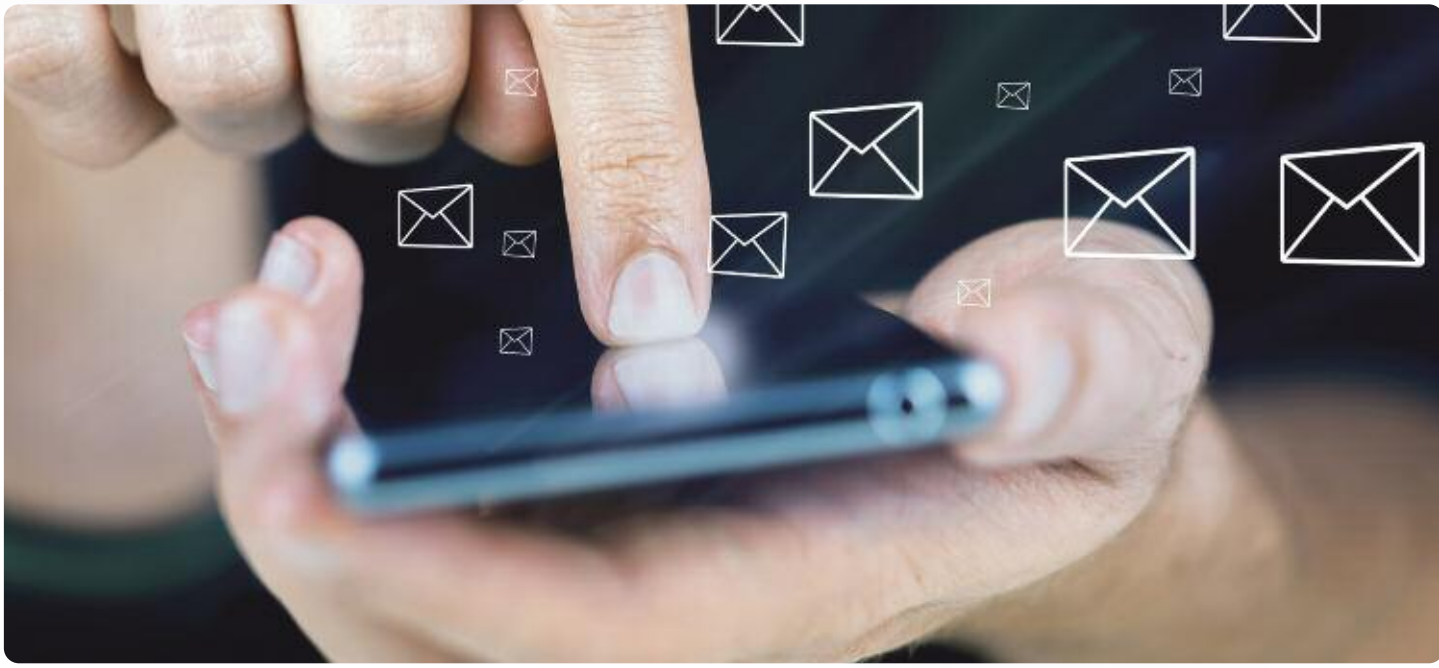
Concernant plus particulièrement les systèmes d'information, la Commission a là aussi émis plusieurs suggestions destinées à renforcer la sécurité de ces systèmes.

Ainsi, elle a proposé de rajouter que chaque intervention d'un fournisseur sur place devait s'effectuer accompagnée d'une personne habilitée et que chaque intervention à distance devait être faite par des liens sécurisés, sous le contrôle d'une personne habilitée.

Enfin, il a été tenu compte de l'observation de la Commission qui estimait que l'accord formel qui précise l'objectif, le cadre de l'intervention du responsable interne en charge du suivi de la prestation de maintenance, devait également stipuler que le prestataire et les membres de son personnel n'agissent que sous le contrôle du responsable de traitement ou de son représentant.

8

LES DELIBERATIONS PORTANT RECOMMANDATION



En application de l'article 2 de la Loi n° 1.165 du 23 décembre 1993, la Commission a adopté en 2019 deux délibérations portant recommandation.

RECOMMANDATION SUR LES MODALITÉS DE DÉPÔT ET LA DURÉE DE CONSERVATION DES COOKIES ET AUTRES TRACEURS SUR LES TERMINAUX D'UTILISATEURS DE RÉSEAUX DE COMMUNICATION ÉLECTRONIQUE

Dans sa délibération n° 2019-083 du 15 mai 2019 la Commission a souhaité préciser dans une recommandation les grands principes applicables aux modalités de dépôt des cookies et autres traceurs sur les terminaux d'utilisateurs de réseaux de communication électronique, et aux durées de conservation de ceux-ci.

Les cookies peuvent être définis tels de petites suites d'informations déposées dans le terminal d'un utilisateur par le serveur du site Internet visité par ce dernier et/ou par un serveur tiers. En fonction de leur nature, ils peuvent concourir à différents objectifs : cookies permettant le fonctionnement du site, cookies permettant une analyse du comportement de l'internaute, cookies publicitaires, cookies de réseaux sociaux...

Par ailleurs, les cookies strictement nécessaires au fonctionnement d'un site Internet peuvent être déposés dans le terminal d'un utilisateur sans recueil de son consentement. Les autres cookies doivent être acceptés par les internautes avant leur dépôt. En cas de refus, le site doit demeurer accessible et fonctionnel.

Ainsi, la Commission a rappelé la nécessité d'insérer un bandeau apparaissant dès l'arrivée d'un Internaute sur le site visité. Elle a également demandé qu'aucun cookie autre que nécessaire au fonctionnement ne soit déposé dans le terminal de l'utilisateur sans que ce dernier ait donné son consentement. A défaut, son consentement serait vicié, d'autant plus que certains cookies tiers peuvent transmettre des informations à des entités autres que l'éditeur du site visité.

A cet égard, elle a tenu à préciser que le bandeau ne doit pas être uniquement à des fins informatives mais doit permettre l'approbation ou la désactivation du dépôt de cookies directement sur le site par une action positive de la personne concernée, si possible par typologie de cookie (publicitaires, analytiques, réseaux sociaux, etc.) avec une option

permettant un refus en une fois. Une information indiquant aux internautes comment paramétrer son/ses navigateur(s) ne remplit pas ces conditions.

Enfin, la Commission a rappelé que pour qu'un consentement soit valable, la qualité de l'information donnée à la personne concernée est essentielle. Il doit également pouvoir être retiré facilement par l'internaute.

S'agissant du transfert d'informations vers un pays ne disposant pas d'un niveau de protection adéquat, la Commission a souhaité rappeler que des cookies tiers peuvent communiquer des informations à leurs éditeurs, qui ne sont pas les éditeurs du site. Il peut s'agir par exemple de certains cookies analytiques (exemple : Google Analytics), publicitaires, ou proposés par les réseaux sociaux (exemple : Facebook Connect), voire même de certains cookies techniques mis à disposition par des sociétés tierces (exemple les recaptcha de Google).

Les sociétés destinataires peuvent être situées dans un pays ne disposant pas d'un niveau de protection adéquat, tels que les Etats-Unis d'Amérique. Monaco n'étant pas couvert par l'accord dit « *Privacy Shield* » liant l'Union Européenne et les Etats-Unis et la Suisse et les Etats-Unis, aucune communication d'informations ne peut être effectuée sans la pleine information des personnes concernées et le recueil de leur consentement spécifiquement à cette fin ; en effet, il s'agit alors d'un transfert vers un pays n'assurant pas un niveau de protection adéquat au sens du deuxième alinéa de l'article 20 de la Loi n° 1.165.

RECOMMANDATION SUR LA SÉCURITÉ DEVANT ENTOURER LES CARTES DE PAIEMENT EN MATIÈRE DE VENTE DE BIENS OU DE FOURNITURE DE SERVICES À DISTANCE AINSI QUE LES SITES WEB

Eu égard au nombre croissant de responsables de traitement effectuant des formalités relatives à la mise en œuvre de sites Internet de vente en ligne, la Commission a souhaité préciser les grands

principes applicables à la sécurité devant entourer les cartes de paiement en matière de vente de biens ou de fourniture de services à distance ainsi que les sites web.

Cette recommandation a donné lieu à la délibération n° 2019-084 du 15 mai 2019.

S'agissant dans un premier temps des cartes bancaires, l'utilisation de moyens de paiements en ligne et la conservation de numéro de cartes bancaires doivent faire l'objet de mesures de traçabilité permettant de détecter a posteriori tout accès illégitime aux données et de l'imputer à la personne ayant accédé illégitimement à ces données.

Le responsable de traitement doit ainsi prendre les mesures organisationnelles et techniques appropriées afin de préserver la sécurité, l'intégrité et la confidentialité des numéros de cartes bancaires contre tout accès, utilisation, détournement, communication ou modification non autorisés en recourant à des systèmes de paiement sécurisés conformes à l'état de l'art et à la réglementation applicable. Ces données doivent être notamment chiffrées par l'intermédiaire d'un algorithme réputé fort.

En ce qui concerne les sites web et la sécurité des traitements, il est rappelé que le responsable de traitement doit notamment s'assurer :

➢ que les utilisateurs s'authentifient individuellement avec un identifiant et un mot de passe réputé fort, ou par tout autre moyen d'authentification apportant au moins le même niveau de sécurité ;

➢ que les habilitations et les mots de passe soient régulièrement mis à jour afin de garantir que seules les personnes habilitées puissent accéder aux données nécessaires à la réalisation de leurs missions ;

➢ que les mesures techniques déployées garantissent la sécurité des données stockées ou échangées, en particulier lors de communications sur Internet ;

➢ de la mise en place d'un mécanisme de journalisation des accès et opérations effectués, et de conservation des données de journalisation pendant une durée de un an à compter de leur collecte.

9

SECTEUR PRIVE : 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 bien particulières ont suscité des discussions au cours de l'année 2019.

INFRACTIONS BOURSIÈRES ET ABUS DE MARCHÉ DES PERSONNES POTENTIELLEMENT INITIÉES

La Commission a eu à examiner plusieurs demandes d'autorisations relatives à la mise en œuvre de traitements ayant pour finalité le contrôle des infractions boursières et des abus de marchés par des personnes potentiellement initiées.

En effet la Loi n° 1.462 du 28 juin 2018 renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption a notamment modifié l'article 49 de la Loi n° 1.338 sur les activités financières afin de durcir la législation en matière de surveillance des opérations bancaires et boursières en prévoyant désormais qu'« *Est puni de deux ans d'emprisonnement et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal dont le montant peut être porté jusqu'au décuple du montant du profit éventuellement réalisé sans que l'amende puisse être inférieure à ce même profit, le fait, pour toute personne de réaliser une opération, de passer un ordre ou d'adopter un comportement qui :*

- *donne ou est susceptible de donner des indications trompeuses sur l'offre, la demande ou le cours d'un instrument financier ou qui fixe ou est susceptible de fixer à un niveau anormal ou artificiel le cours d'un instrument financier ;*

- *affecte le cours d'un instrument financier, en ayant recours à des procédés fictifs ou à toute autre forme de tromperie ou d'artifice afin d'entraver le fonctionnement régulier d'un marché d'instruments financiers en induisant autrui en erreur.* »

Ainsi, le produit des infractions prévues à l'article 49 de la Loi n° 1.338 pouvant être qualifié de biens, capitaux ou revenus d'origine illicite au sens de l'article 218-3 du code pénal monégasque, il pourrait donner lieu à un déclaration de soupçon auprès du SICCFIN en application de l'article 36 de Loi n° 1.362

A ce titre, le secteur bancaire exerce une vigilance constante afin de s'assurer que les opérations de la clientèle ne relèvent pas de l'une des opérations visées par la Loi précitée. Ce traitement est ainsi mis en œuvre à des fins de surveillance et est donc soumis au régime de l'autorisation préalable de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives.

Dans le cadre des demandes qui lui ont été soumises, la Commission, pleinement consciente de la nécessité qui s'attache à contraindre efficacement toute pratique pouvant relever de faits pénalement sanctionnables, a toutefois tenu à rappeler que les traitements mis en œuvre en matière de lutte contre les abus de marchés se devaient de respecter strictement le cadre légal applicable, s'agissant notamment du quantum des informations traitées, de leur durée de conservation, et des destinataires potentiels desdites informations.

MESURES DE VIGILANCE EN MATIÈRE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX

En 2019 ont également été soumises à la Commission des demandes d'autorisations portant sur des traitements, ou des transferts d'informations nominatives vers des pays ne disposant pas d'un niveau de protection adéquat, dont la finalité était de soumettre aux mesures de vigilance prévues en matière de lutte contre le blanchiment de capitaux, des catégories de personnes dont le droit interne ne prévoit pas qu'elles en fassent l'objet.

L'examen de ces dossiers a été une nouvelle fois l'occasion pour la CCIN de préciser que les vérifications en matière de LAB étant potentiellement intrusives, il importait qu'elles ne soient appliquées qu'à l'égard des personnes qui y sont légalement soumises.

Ainsi, dans le cadre de l'examen de ces dossiers, lorsque l'un des responsables de traitement a indiqué que la mise en œuvre des diligences prévues en matière de lutte contre le blanchiment de capitaux répondait à une « *attente réglementaire* » la Commission a rappelé que seules les personnes expressément visées par la Loi n° 1.362 du 3 août 2009, modifiée, et ses textes d'application sont susceptibles de faire l'objet des diligences qui s'y rapportent.

A cet égard, s'agissant plus particulièrement des salariés des entités assujetties à la Loi n° 1.362, l'article 30 de l'Ordonnance n° 2.318 fixant les conditions d'application de ladite Loi précise que « *les professionnels [...] prennent en compte, dans le recrutement de leur personnel, selon le niveau des responsabilités exercées, les risques au regard de la lutte contre le blanchiment de capitaux et le financement du terrorisme.* »

De même aucune disposition de droit interne ne soumet les salariés des prestataires des entités assujetties aux mesures de vigilance en matière de LAB.

En outre la justification fondée sur l'intérêt légitime du responsable de traitement n'a également pas été retenue par la Commission dans la mesure où le traitement envisagé était de nature à méconnaître l'intérêt ou les droits des personnes concernées.

A l'issue de l'examen de ces dossiers la Commission a donc refusé la mise en œuvre des traitements, et des transferts d'informations y afférents.

LES DISPOSITIFS DE CONTRÔLE D'ACCÈS DANS LES IMMEUBLES D'HABITATION

De nombreux dispositifs de contrôle d'accès par badges magnétiques sont chaque année soumis à l'autorisation préalable de la Commission. Mis en place la plupart du temps sur le lieu du travail, ces dispositifs reposent dans la nécessaire identification des personnes aux fins de surveiller ceux qui pénètrent dans les locaux ou dans certaines zones à accès restreint. La surveillance s'étend donc aussi bien à l'identité des personnes concernées qu'à la date, l'heure et la porte par laquelle elles ont pu accéder à ces locaux.

Si ces personnes sont très souvent des employés, quelle que soit la nature de leur emploi (salariés

et consultants en mission), la Commission a eu à se prononcer pour la première fois en 2019 sur l'installation d'un tel dispositif dans deux immeubles qui concernaient avant tout les résidents desdits immeubles.

Elle a ainsi décidé d'adapter les règles établies dans sa délibération n° 2010-43 du 15 novembre 2010 portant recommandation sur les dispositifs de contrôle d'accès sur le lieu de travail mis en œuvre par les personnes physiques ou morales de droit privé afin de tenir compte du droit qu'a tout résident d'un immeuble d'habitation au respect de sa vie privée.

Alors qu'elle autorise habituellement, parmi les données relatives à l'identité d'une personne, la collecte des noms et prénoms, elle a en effet estimé que pour un dispositif installé dans un immeuble d'habitation, seul le numéro des badges des résidents devait être traité, afin que ces derniers ne soient pas directement identifiables par ledit dispositif.

La Commission a toutefois tenu à préciser qu'en cas de besoin, les détenteurs de badges pourront être identifiés par rapprochement avec les traitements contenant leur identité.

VIDÉOSURVEILLANCE DANS LES RESTAURANTS ET BARS

La Commission considère qu'un restaurant ou un bar est avant tout un lieu que les clients fréquentent pour passer un bon moment, discuter ou se détendre.

Ils s'attendent légitimement à ne pas être filmés pendant ces moments qui relèvent de leur sphère privée, afin de ne pas se sentir observés de manière permanente et inopportune.

La Commission interdit donc, lorsque cela est le cas, les caméras qui filment les clients lorsqu'ils sont à table ou au comptoir.

En outre, le dispositif de vidéosurveillance ne doit pas conduire à contrôler le travail des employés.

La Commission interdit donc les caméras qui filment les zones de travail de ces derniers, comme par exemple les plans de travail dans les cuisines.

Enfin, les toilettes et les lieux privatifs mis à disposition des employés, tels qu'une salle de repos ou les vestiaires, ne peuvent pas être filmés.

En revanche, les caméras peuvent filmer :

- les portes d'entrée et de sorties, en faisant attention toutefois à ne filmer que la surface strictement nécessaire ;
- les zones de stockage, les réserves, les caves ;
- les caisses ;
- les extérieurs, à condition toutefois de ne filmer que les espaces exploités par le responsable de traitement ;
- le parking intérieur, extérieur et/ou souterrain.

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.

AU NIVEAU NATIONAL ET RÉGIONAL

13ème Journée européenne de la protection des données

Parce que « *La protection des données c'est toute l'année* » la CCIN a décidé début 2019 d'offrir chaque jour de l'année sur son site internet, www.ccin.mc, un conseil destiné à sensibiliser les particuliers et les professionnels au respect de la vie privée et des informations nominatives.

Les internautes ont ainsi pu lire qu'il était important de créer des profils séparés « *personnels* » et « *professionnels* » sur les réseaux sociaux, que tout mot de passe doit être composé de caractères minuscules, de caractères majuscules, de chiffres et de caractères spéciaux ou encore qu'il convient de mettre à jour régulièrement ses logiciels, pare-feu et anti-virus sur ses équipements.

Cette campagne a été réalisée à l'occasion de la 13ème Journée européenne de la Protection des Données Personnelles. Créée en 2007 par le Conseil de l'Europe et relayée par la Commission européenne, cette journée a, comme son nom l'indique, pour objectif principal d'informer les personnes sur les risques liés à la protection de leurs données à caractère personnel et leurs droits en la matière.

Cette journée est célébrée le 28 janvier de chaque année. Ce jour n'a pas été choisi au hasard, puisqu'il correspond à la date d'ouverture à la signature des Etats membres et à l'adhésion des Etats non membres de la Convention 108 du Conseil de l'Europe, premier instrument international contraignant ayant pour objet la protection des personnes contre l'usage abusif du traitement automatisé de données à caractère personnel. Membre du Conseil de l'Europe, Monaco fait partie des signataires de ladite Convention depuis 2008.

Participation à la 19ème édition des Assises de la Sécurité

Rendez-vous annuel incontournable de la cybersécurité, la 19ème édition des Assises de la Sécurité et des Systèmes d'Information s'est tenue du 9 au 12 octobre 2019, au Grimaldi Forum de Monaco.

Cette année, les visiteurs des Assises ont pu accéder à 150 ateliers, keynotes et tables-rondes sur des sujets de cybersécuité. Les grandes institutions cyber étaient présentes telles que la plateforme de l'Etat français cybermalveillance.gouv.fr.

Grande nouveauté de cette édition, les Assises ont accueilli pour la 1ère fois à Monaco un village start-up avec huit jeunes entreprises emblématiques du dynamisme du secteur de la cybersécurité.

Après une année 2019 émaillée par de nombreuses cyberattaques qui ont touché plusieurs grands groupes européens, le thème phare de cette édition était inévitablement la détection des cybermenaces. Lors de son discours d'ouverture, le directeur général de l'Agence Nationale française de la Sécurité des Systèmes d'Information (ANSSI), Guillaume POUPARD a souligné qu' : « *il faut arrêter de faire peur et apporter des solutions technologiques, notamment dans la détection des cybermenaces* ».

Ainsi, les débats se sont articulés autour de sujets majeurs : l'identification de la threat intelligence (outils de profilage des cyberattaquants), le cloud computing, l'arrivée de la 5G et ses impacts géopolitiques, la protection des données, la cryptographie, l'intelligence artificielle, la blockchain ou encore la sécurité des objets connectés (IoT).

AU NIVEAU INTERNATIONAL AUPRÈS DES ACTEURS DE LA PROTECTION DES INFORMATIONS NOMINATIVES

Conférence européenne des Autorités de protection des données en Géorgie

La 29ème édition de la Conférence européenne des Autorités de protection des données, plus communément appelée Conférence de printemps, s'est tenue les 9 et 10 mai 2019 à Tbilissi, capitale de la Géorgie, en présence de deux agents du Secrétariat de la CCIN.

Organisée juste un an après l'entrée en vigueur du Règlement général sur la protection des Données (RGPD), cette réunion a permis aux membres des Autorités présentes d'assister à des débats sur les réalisations et les défis liés à la mise en œuvre et à l'application de ce « *standard de référence* ». Dans ce cadre, différentes actions effectuées par les Autorités ont été abordées,

notamment la mise en place d'un logiciel permettant la réalisation d'analyses d'impact en 16 langues, l'organisation de réunions d'information avec de nombreux délégués à la protection des données et de cours de formation en ligne, ou encore l'accompagnement des collectivités territoriales et des très petites entreprises. Ces premiers retours d'expérience donnent ainsi la possibilité à la Commission de cerner au mieux les futures actions qui pourraient potentiellement être mises en œuvre lorsque les principes tirés du RGPD seront à appliquer en Principauté, dans le cadre de l'entrée en vigueur de la nouvelle Loi monégasque de protection des données personnelles.

La portée extraterritoriale du RGPD et les mécanismes de coopération ont ainsi notamment été évoqués. L'Autorité fédérale suisse de protection des données personnelles a mis en exergue cette situation, où une large partie des entreprises du pays est soumise au Règlement européen, et de facto sujette aux investigations et potentielles condamnations prévues par le RGPD. L'exemple suisse, qui se révèle en de nombreux points similaire à la situation de Monaco, permet ainsi à la Commission de mieux cibler les attentes et futurs enjeux à relever dans le cadre de cette période transitoire, où les entreprises territorialement implantées à Monaco ou en Suisse restent pour autant soumises aux Lois nationales de leur pays respectif : l'intérêt de modifier la Loi nationale afin de se rapprocher des nouveaux standards du RGPD et de la Convention 108 révisée et ainsi, tout au long de cette période de transition, être en capacité de trouver des solutions de coopération avec les Autorités européennes de protection des données.

ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES

12ème Conférence annuelle et 13ème Assemblée générale de l'AFAPDP à Dakar

Comme chaque année depuis 2008, l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) s'est réunie pendant deux jours afin de préciser les positionnements et la stratégie d'action du réseau francophone dans le contexte du développement de l'usage des technologies de l'information et de la communication. Deux agents de la CCIN étaient présents.

Organisée à Dakar le 17 septembre sur le thème du « *Citoyen Numérique* », la conférence annuelle a permis d'évoquer des sujets aussi divers que la digitalisation des faits d'état civil, la portabilité des données et l'anonymat sur les réseaux sociaux.

Par ailleurs, la veille, lors de son Assemblée Générale, l'Association a accueilli en son sein un nouveau membre, le Commissaire à l'information (OIC) de l'île de Jersey, et deux observateurs, la Conférence Internationale des Commissaires à la Protection des Données Personnelles et à la Vie Privée (CICPDVP) et l'Autorité de Régulation des Télécommunications (ART) du Cameroun.

Elle a également élu son nouveau bureau qui est composé pour les 3 prochaines années comme suit :

- Présidence : INPDP (Tunisie) ;
- Vice-Présidence : IDP (Albanie) ;
- Vice-Présidence : CIL (Burkina Faso) ;
- Vice-Présidence : CNDP (Cap-Vert) ;
- Secrétariat Général : CNIL (France).

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

Elle compte désormais 21 membres.

Participation aux réunions du Groupe de Berlin organisées en Slovénie et en Belgique

Les 9 et 10 avril puis les 10 et 11 octobre 2019, se sont tenues respectivement à Bled, en Slovénie, et à Bruxelles, les 65ème et 66ème réunions de l'« *International Working Group on Data Protection in Telecommunications* », plus communément appelé « *Groupe de Berlin* », auxquelles deux agents de la CCIN ont participé.

Au programme, des sujets d'actualité allant des réseaux sociaux à la portabilité des données, en passant par la technologie blockchain ou encore les appareils contrôlés par la voix.

Ces discussions fructueuses ont abouti à l'adoption de deux résolutions, la première sur les objets connectés pour les enfants et la deuxième sur la protection des mineurs sur internet.

Par ailleurs, plusieurs travaux ont été présentés dont un document de travail sur la traçabilité et l'analyse statistique détaillée de la navigation sur internet auquel la CCIN a contribué et qui devrait donner lieu l'année prochaine à un texte de référence.

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

11

FICHES PRATIQUES

DU BON USAGE DE L'ARCHIVAGE

Pour les personnes physiques ou morales, l'archivage des données dans le cadre de leur activité professionnelle peut répondre à des besoins ou impératifs divers qui vont de la simple mesure organisationnelle de stockage de données à la nécessité juridique ou bien encore à la préservation de l'histoire d'une entreprise.

Or, l'idée même d'archivage peut sembler a priori aller à l'encontre des principes de protection des données personnelles, et notamment le droit à l'oubli (ou la nécessité de conserver les données pour une durée déterminée, et donc limitée) ou encore le principe d'interdiction du détournement de finalité.

Ainsi, face aux impératifs de la Loi n° 1.165 du 23 décembre 1993, modifiée, de multiples problématiques juridiques se posent, et notamment :

- quelle est la finalité d'un traitement comportant des archives ?
- le fait de procéder à l'archivage de données contenues dans un ou plusieurs traitements constitue-t-il un détournement de finalité ?
- comment appliquer les principes d'adéquation et de pertinence des données collectées en matière d'archives ?
- combien de temps peut-on licitement conserver des données archivées ?
- de quels droits les personnes concernées disposent-elles face à l'archivage de leurs informations nominatives ?
- comment assurer la confidentialité et la sécurité des données archivées ?

Qu'est-ce que l'archivage ?

D'après le dictionnaire Larousse, les « *archives* » *sont l'« ensemble des documents relatifs à l'histoire d'une ville, d'une famille, etc., propres à une entreprise, à une administration, etc.* ».

Il ressort de cette définition que les archives peuvent revêtir plusieurs natures.

- Archives publiques, privées ou personnelles

Tout d'abord, les **archives dites publiques** sont encadrées, à Monaco, par la Section II de l'Ordonnance n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré qui concerne les documents administratifs produits ou détenus par les Services de l'Administration monégasque.

La notion d'archives peut également viser les **archives domestiques** de particuliers souhaitant conserver des documents dans le cadre de leurs activités privées et personnelles : photos, fiches de paie, documents administratifs divers, etc.

Enfin, les responsables de traitement peuvent avoir intérêt à stocker, ou être légalement tenus de conserver un certain nombre de données. Ce stockage revêt alors un **caractère professionnel :** documents commerciaux, comptables, fiscaux, etc. Dans certains cas, il peut également s'agir de préserver l'histoire de l'entreprise. Seule cette troisième catégorie d'archives dîtes « *professionnelles* » est concernée par cette fiche pratique.

- Archives papier ou numériques

Traditionnellement, la conservation des archives se fait par voie papier. Toutefois, avec l'entrée dans la Société numérique, le stockage de données et documents s'est dématérialisé.

Cette dématérialisation pose plusieurs questions, et notamment :

- la question de l'intégrité des données conservées ;
- la valeur juridique des documents dématérialisés.

En France, l'Afnor a émis plusieurs normes qui constituent, à l'heure actuelle, les règles de l'art en matière d'archivage électronique, à savoir :

- la norme NF Z 42-013 relative à « *la conception et l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes* ». Cette norme date de 1999 mais a été révisée en 2009 afin d'élargir le périmètre de la norme à tous les types de supports numériques et non plus aux seuls disques optiques numériques non-réinscriptibles. Elle a donné naissance en 2012 à la norme internationale ISO 14641-1.

- La norme NF Z42-026 relative aux « *Définitions et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations* », parue dans sa première version en mai 2017. Si cette norme concerne avant tout la numérisation de documents d'activité, elle permet néanmoins d'adapter les exigences en fonction de l'enjeu juridique porté par le document original. Ces exigences pourront donc être modulées selon le degré de fidélité formelle recherché, mais doivent être formalisées dans une convention de numérisation.

Toutefois, pour ce qui est des archives professionnelles des entreprises, ces normes n'ont aucune force contraignante, que ce soit en France ou à Monaco.

Quoi qu'il en soit, si la Loi n° 1.165 du 23 décembre 1993, modifiée, s'applique aux traitements automatisés d'informations nominatives, ses principes, à l'exception de ceux contenus dans les chapitres relatifs aux obligations déclaratives, s'appliquent également à la conservation des documents papier sous forme de fichier même non automatisé.

- Archives courantes, intermédiaires ou définitives

En matière d'archives publiques, une distinction est traditionnellement faite entre les notions d'archives courantes, intermédiaires et définitives.

Cette distinction peut être transposée aux archives professionnelles.

Ainsi, dans sa délibération n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique dans le secteur privé des données à caractère personnel, la Commission Nationale de l'Informatique et des Libertés (CNIL) définit ces notions de la manière suivante :

- « *par **archives courantes**, il convient d'entendre les données d'utilisation courante par les services concernés dans les entreprises, organismes ou établissements privés (par exemple les données concernant un client dans le cadre de l'exécution d'un contrat)* ;
- *par **archives intermédiaires**, il convient d'entendre les données qui présentent encore pour les services concernés un intérêt administratif, comme par exemple en cas de contentieux, et dont les durées de conservation sont fixées par les règles de prescription applicables* ;
- *par **archives définitives**, il convient d'entendre exclusivement les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction* ».

• *Les archives courantes*

A la lumière de ces définitions, il convient de constater que les « *archives courantes* » correspondent en réalité aux données et fichiers couramment exploités par les responsables de traitement dans le cadre de leur activité professionnelle : fichiers de gestion de la clientèle, des ressources humaines, etc.

Ces traitements sont soumis aux dispositions de la Loi n° 1.165 du 23 décembre 1993, modifiée, comme tout traitement d'informations nominatives. Par ailleurs, en fonction de leur finalité, il conviendra, le cas échéant, de se rapporter aux diverses délibérations portant recommandation émises par la Commission.

• *Les archives intermédiaires*

Les « *archives intermédiaires* » ne contiennent pas des données utilisées dans la gestion courante des activités de l'entreprise, mais qui doivent néanmoins être conservées pour divers motifs, à savoir, notamment :

- à des fins de preuve, conformément aux délais de prescription légale : ex. contrats commerciaux ou de travail, pièces utilisées dans le cadre de procédures judiciaires en cours, données utiles pour la détection d'éventuelles infractions prévues par le Code pénal (ex. blanchiment d'argent), etc. ;
- conformément à une obligation légale : ex : les obligations particulières de vigilance et de traçabilité des opérations effectuées imposées à certains établissements bancaires ou assimilés, notamment, par la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, modifiée, et son Ordonnance Souveraine d'application.

• *Les archives définitives*

Les archives définitives de l'entreprise sont l'ensemble des données et documents conservés sans limitation de durée.

Dans la mesure où elles sont susceptibles de contenir des informations nominatives, il convient d'examiner sous quelles conditions ce type de traitements peut être compatible avec les dispositions de la Loi n° 1.165 du 23 décembre 1993, modifiée, et notamment son article 9 qui, dans une lecture a contrario, autorise la conservation illimitée de données « *à des fins historiques, statistiques ou scientifiques* », ou dans les cas prévus par la Loi.

Les principes en matière d'archivage

• *Un archivage sélectif*

Comme cela a été précédemment exposé, archiver ses données peut répondre à une nécessité juridique pour l'entreprise.

Toutefois, lorsque cette nécessité d'archivage répond à une obligation légale, le responsable de traitement doit veiller à archiver uniquement les données utiles au respect de ladite obligation, ou pour faire valoir un droit en justice.

Il doit donc impérativement faire un tri parmi la totalité des données collectées pour ne garder que les seules données indispensables.

Exemple de la « *Gestion et supervision de la messagerie professionnelle* » :

Le responsable de traitement devra, conformément à la délibération n° 2015-111 du 18 novembre 2015 de la Commission, supprimer les données liées à l'administration de la messagerie électronique (compte individuel et carnet d'adresses) au bout de 3 mois maximum après le départ de l'utilisateur et les données de connexion au bout d'un an, mais pourra archiver le contenu des messages émis et reçus jusqu'à ce que la conservation desdits messages ne soit plus nécessaire.

• *Un mode d'archivage libre*

Même si le responsable de traitement a une obligation légale de conserver certaines données, le choix du mode d'archivage est laissé à son appréciation. Il peut donc choisir entre une des deux méthodes suivantes :

- dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter ;

- dans une base d'archive spécifique, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaître en raison de leurs fonctions (par exemple, le service du contentieux).

En ce qui concerne les archives définitives, à savoir les données présentant un intérêt historique, scientifique ou statistique, il est recommandé de les conserver sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter (par exemple, le service des archives).

Quid de la finalité et des fonctionnalités du traitement

Conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, un traitement d'archives doit, au même titre que tout traitement d'informations nominatives, disposer d'une finalité « *déterminée, explicite et légitime* ».

Ainsi, une finalité telle que l'« *archivage de données* » ne saurait être considérée comme répondant à cette exigence légale. Il convient en effet de déterminer le but d'un tel archivage, en fonction duquel pourront ensuite être fixées la durée de conservation des données, les règles régissant l'accès à ces dernières, etc.

La finalité du traitement dépendra de la nature des données qui le composent et à cet égard, il convient de distinguer le traitement dit « *mixte* » du traitement uniquement composé d'archives.

• *Le traitement mixte*

Un traitement mixte est un traitement comportant à la fois des données d'utilisation courante ainsi que des archives intermédiaires et qui, en conséquence doit disposer d'une finalité globale justifiant du traitement de ces deux types de données.

Ex. Gestion et supervision de la messagerie, gestion des ressources humaines, gestion du fichier clients/fournisseurs, gestion des dossiers patients, etc.

Le traitement « *mixte* » comportant à la fois des archives courantes et intermédiaires, il est soumis aux formalités légales habituelles, sous réserve qu'il soit automatisé.

A ce titre, il convient de préciser, dans le cadre de ses **fonctionnalités**, les objectifs de l'archivage intermédiaire des données venant s'ajouter aux fonctionnalités liées à l'exploitation courante du traitement.

Exemple de la « *Gestion et supervision de la messagerie professionnelle* » :

Dans un établissement bancaire ou assimilé, les messages électroniques des collaborateurs peuvent être conservés durant plusieurs années notamment à des fins de traçabilité des opérations financières, ou en cas de soupçons d'activités illicites.

Dans ce cas, les messages récents peuvent être stockés dans la messagerie interne du collaborateur pendant une courte période (1 an selon la délibération n° 2015-111 du 18 novembre 2015), puis être automatiquement effacés de sa messagerie, et conservés dans un serveur distinct jusqu'à l'expiration du délai nécessaire.

Pour autant, quel que soit leur lieu de stockage, l'ensemble de ces données fait l'objet d'un seul et même traitement ayant pour finalité « *Gestion et supervision de la messagerie électronique* ».

Toutefois, une des fonctionnalités liées à un tel archivage intermédiaire serait la préservation de preuve en cas d'infractions, ou encore la conservation de données à des fins de traçabilité des transactions financières. Par ailleurs, en ce qui concerne l'utilisation courante de la messagerie, les fonctionnalités y afférentes seraient, notamment, l'échange de messages électroniques en interne ou avec l'extérieur, l'historisation des messages entrants et sortants, la gestion des contacts, etc.

Enfin, les accès seront conférés tant aux personnes exploitant la messagerie dans le cadre d'une utilisation professionnelle courante (ex. utilisateurs, administrateur informatique), qu'aux personnes habilitées à exploiter les données conservées au titre des archives intermédiaires (ex. service juridique, Compliance, Direction).

- ***Le traitement uniquement composé d'archives***

Si le traitement est composé uniquement d'archives, qu'elles soient intermédiaires, ou définitives, sa finalité devra décrire avec précision le motif de cet archivage dans un traitement distinct.

Ex. Gestion du contentieux, conservation de données à des fins historiques, etc.

Exemple de la « *Gestion du contentieux* » :

A des fins de preuves dans le cadre de contentieux, des pièces et données issues de divers traitements (Gestion des ressources humaines, dispositif de pointage, système d'alerte professionnel, messagerie professionnelle, etc...) peuvent être extraites afin d'être exploitées dans le cadre d'un traitement distinct, ayant par exemple pour finalité « *Gestion des contentieux* », accessible uniquement par le service juridique de l'entreprise.

Il s'agit alors d'un nouveau traitement, dont les modalités d'exploitation sont distinctes de celles des traitements dont les données archivées sont issues (ex. Gestion des ressources humaines).

Automatisés, ils sont soumis aux formalités légales prévues par les articles 6 et suivants de la Loi n° 1.165 du 23 décembre 1993, modifiée.

• *Sur le risque de détournement de la finalité*

L'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, dispose que « *les informations nominatives doivent (...) ne pas être traitées ultérieurement de manière incompatible avec [la] finalité [pour laquelle elles ont été collectées]* ».

Par conséquent, lorsque des données sont initialement collectées pour une finalité déterminée (ex. gestion de la messagerie) et ultérieurement traitées à d'autres fins dans le cadre d'un traitement distinct (ex. contentieux), il appartient tout d'abord au responsable de traitement de s'interroger sur la compatibilité de ce traitement avec la finalité pour laquelle les données ont été initialement collectées.

A cet égard, il convient de rappeler qu'aux termes de l'article 10-1 susvisé, les informations nominatives doivent être « *collectées et traitées loyalement et licitement* ».

Ainsi, il y aura collecte déloyale et détournement de finalité lorsque, sous couvert d'une finalité première (ex. gestion de la messagerie professionnelle), les données sont exploitées à d'autres fins (ex. surveillance des salariés).

De plus, à travers l'obligation d'information des personnes concernées mise à la charge des responsables de traitement par l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée, le législateur a souhaité entériner un principe de transparence relatif aux traitements de données à caractère personnel.

Par conséquent, aucune information nominative ne saurait être exploitée pour une finalité autre que celle pour laquelle elle a été initialement collectée et/ou traitée, sans que la personne concernée en soit tenue informée. L'archivage de données dans le cadre d'un nouveau traitement devra donc toujours être porté à la connaissance des personnes concernées.

La justification de l'archivage d'informations nominatives

En application des dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993, modifiée, tout traitement d'archives comportant des informations nominatives (intermédiaires ou définitives) peut être justifié, notamment, par :

- le respect d'une obligation légale : les « *livres de commerce* », en application de l'article 13 du Code de commerce ; les documents d'identification des clients pour les transactions sur l'or de plus de 15.000 euros, en vertu de l'article 100 bis E du Code des Taxes sur le Chiffre d'Affaires ; les données relatives aux accès aux lieux de spectacles, conformément à l'article 76 de ce même Code ; les pièces comptables et commerciales sur lesquelles peut s'exercer le droit de communication et de contrôle de la Direction des Services Fiscaux, en application de l'article 66 dudit Code ; etc.

- la réalisation d'un intérêt légitime poursuivi par le responsable de traitement ou son représentant : conservation de documents durant les délais de prescription légale ; conservation de preuves en cas de litige ; préservation de documents historiques, scientifiques ; etc. ; ou

- le consentement de la personne concernée : celui-ci sera apprécié au cas par cas, en tenant compte du lien de subordination éventuel existant entre la personne concernée et le responsable de traitement ou son représentant.

La durée de conservation des données archivées

Aux termes de l'article 10 de la Loi n° 1.165 du 23 décembre 1993, modifiée, « *les informations nominatives doivent être (...) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées ou pour laquelle elles sont traitées ultérieurement* ».

Ainsi, il appartient au responsable de traitement de déterminer la durée de conservation de chaque catégorie de données archivées, en fonction de la finalité du traitement dans le cadre duquel elles sont exploitées.

Cela signifie qu'il devra également mettre en place des mécanismes de purge sélective des données.

S'agissant plus particulièrement des archives définitives, l'article 9 pose le principe de l'interdiction de la conservation illimitée d'informations nominatives, sauf dans les cas prévus par la Loi, ou lorsque lesdites données sont « *traitées à des fins historiques, statistiques ou scientifiques* ».

Ainsi, seules les informations nominatives répondant à ces critères pourront être licitement conservées dans le cadre d'un archivage dit « *définitif* ».

Enfin l'anonymisation de ces données est recommandée, dès lors que le caractère nominatif n'est pas nécessaire à la finalité pour laquelle elles sont archivées (ex. données statistiques).

Information des personnes concernées

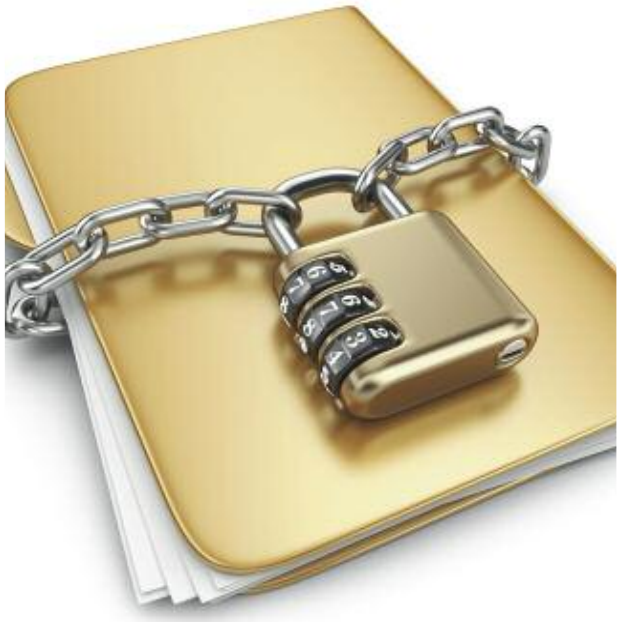
• *Mentions obligatoires*

L'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée, impose aux responsables de traitement une obligation d'information des personnes concernées.

Les traitements d'archives n'y font pas exception.

Ainsi, les personnes dont les informations nominatives sont archivées à des fins professionnelles par des responsables de traitement, personne physique ou morale de droit privé, doivent être informées :

- de l'identité du responsable de traitement ou de son représentant ;
- de la finalité du traitement ;
- de l'identité des destinataires ou catégories de destinataires, le cas échéant ;
- de leurs droits d'opposition, d'accès et de rectification relativement aux informations les concernant ;
- de leur droit de s'opposer à l'utilisation pour le compte de tiers, ou à la communication à des tiers d'informations nominatives les concernant à des fins de prospection, notamment commerciale.



• *Sur les droits d'accès et de rectification des personnes concernées*

L'article 15 de la Loi n° 1.165 du 23 décembre 1993, modifiée, consacre, au bénéfice des personnes concernées, un droit d'accès à leurs informations nominatives exploitées dans le cadre de traitements automatisés ou non automatisés.
Aucun principe de ladite Loi ne permet d'exclure l'application de ce droit en matière d'archives, dès lors qu'elles contiennent des informations nominatives.

De plus, la Loi n° 1.165 du 23 décembre 1993, modifiée, ne prévoit pas d'exception à un tel droit pour ce qui est des archives de données conservées à des fins historiques, statistiques ou scientifiques. Ainsi, le droit d'accès légalement conféré aux personnes concernées s'applique également aux traitements d'archives, quelle qu'en soit la nature (archives intermédiaires ou définitives).

Seul le caractère abusif de demandes de droit d'accès pourra, le cas échéant, dispenser le responsable de traitement de son obligation de réponse, sur décision du Président de la CCIN.

Personnes ayant accès aux informations et destinataires

• *Sur les personnes ayant accès aux traitements et les destinataires*

L'article 17 de la Loi n° 1.165 du 23 décembre 1993, modifiée, dispose que « *le responsable de traitement ou son représentant est tenu de prévoir les mesures techniques et d'organisation appropriées pour protéger les informations nominatives contre (...) la diffusion ou l'accès non autorisé (...)* ».

Il appartient donc à celui-ci de mettre en œuvre des procédures d'habilitation permettant de contrôler l'accès aux divers traitements qu'il exploite.

Ces accès doivent être justifiés, tant par la nature des archives concernées, que par les attributions des personnes habilitées à y accéder.

Ainsi, il convient de distinguer :

- d'une part, l**es archives intermédiaires**, pour lesquelles l'accès devrait être restreint à un ou plusieurs services spécifiques dont les attributions justifient une telle habilitation (ex. service Compliance d'un établissement bancaire ; service juridique ; service des ressources humaines, etc.) ;

- d'autre part, les **archives définitives**, pour lesquelles les accès doivent être ponctuels et motivés. En outre, les demandes d'accès devront être requises auprès de la personne ou du service en charge de la gestion de telles archives.

• Sur les destinataires

Le responsable de traitement est également tenu de s'assurer que tout destinataire potentiel des données archivées est habilité à les recevoir au regard de ses attributions, mais aussi de l'exploitation qu'il souhaite en faire.

Il s'agit d'éviter, d'une part, une atteinte à la confidentialité des données, et d'autre part, un potentiel détournement de finalité.

Ainsi, par exemple, les Autorités judiciaires seront habilitées à recevoir toutes données compilées à des fins de preuves dans le cadre d'un contentieux.

Enfin, ces transferts ou extractions de données devront être sécurisés sur leur support de réception (ex. clé USB, CD ou DVD chiffré).

Mesures de sécurité et de confidentialité des données archivées

Les articles 17 et 17-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, imposent au responsable de traitement (ou à son représentant) une obligation de sécurité et de confidentialité des données qu'il exploite. Cette obligation s'applique également en matière d'archives.

Les trois axes principaux de la sécurité informationnelle sont :

-la confidentialité,
-la disponibilité ; et
-l'intégrité des données.

Les grandes fonctions d'un archivage électronique sécurisé doivent être :

-la collecte de données ;
-le stockage desdites données ;
-la consultation/communication.

A cet égard, il convient de conduire une analyse prospective du système d'archivage afin d'assurer la continuité de ces services, notamment en cas de changement de prestataire ou des supports ou solutions de stockage des données.

• Les différents types de stockage des données

D'un point de vue technique, l'archivage de données dans une entreprise peut être effectué de plusieurs manières. En effet, l'archivage de données n'est rien de plus qu'un stockage des

données répondant à des modalités particulières (accès, durée de conservation, etc.) et disposant, dans certains cas, d'une finalité propre.

Ainsi, des données pourraient être archivées :

- sur un disque dur (local, virtuel, amovible, etc.) ;
- sur un serveur en réseau ;
- en hébergement chez un prestataire ;
- via un service de Cloud computing ;
- sur un support physique distinct sécurisé, éventuellement stocké dans un lieu sécurisé (type coffre).

Le choix des modalités de stockage dépendra du type d'archives concernées (intermédiaires, définitives), ainsi que des contraintes organisationnelles de l'entreprise.

Les modalités techniques de protection de la sécurité et de la confidentialité des données archivées

• *Le contrôle d'accès aux données : séparation logique et séparation physique*

Comme indiqué précédemment, il convient que la procédure d'accès aux données archivées prenne en compte tant la nature des archives concernées, que les attributions des personnes susceptibles d'y avoir accès.

A cet égard, une séparation logique des données parait être la mesure minimale afin de garantir la confidentialité des données archivées. Ainsi, seules les personnes disposant des habilitations informatiques nécessaires pourront accéder aux données dont s'agit.

Concernant plus particulièrement les archives définitives, il convient de rappeler que ces dernières n'ont pas vocation à être exploitées dans le cadre des activités courantes de l'entreprise. De ce fait, il pourrait être recommandé qu'elles soient stockées non pas dans le système d'information de l'entreprise, mais sur un support distinct.

Il pourrait par exemple s'agir d'un stockage par le biais d'un système d'archivage DVD robotisé, ou encore d'un stockage sur disques virtuels.

Enfin, il est recommandé une traçabilité des accès afin d'identifier, le cas échéant, l'origine d'une faille de sécurité ou d'une atteinte à l'intégrité des données.

• La sauvegarde des données

La sauvegarde des données archivées peut être nécessaire afin de préserver l'intégrité des archives concernées en cas de panne ou de faille informatique de quelque nature que ce soit.

Cette sauvegarde devra être effectuée sur un support sécurisé, et les données devront être chiffrées.

Des disques à auto-chiffrement (Self-Encrypting Drive) peuvent par exemple assurer la sécurité des données pendant toute la durée de vie du disque. Cette technologie est désormais accessible pour tout responsable de traitement.

• Le chiffrement des données

Afin de préserver la confidentialité, les fichiers et dossiers contenant les données archivées doivent être chiffrés sur leur support de stockage, mais également en cas de transfert desdites données, quelle qu'en soit la nature.

Ce premier niveau de chiffrement peut être doublé d'un second niveau de chiffrement, plus global, des postes de travail ou encore des disques durs sur lesquels les données sont susceptibles d'être stockées.

- *La consultation des archives par le biais d'équipements mobiles*

En cas d'accès aux données archivées par le biais d'équipements mobiles, il conviendra de garantir la sécurité de cette consultation :

- en mettant en place une connexion sécurisée ;
- par le chiffrement des données consultables, y compris lors de leur éventuel transit ;
- par une gestion stricte des équipements mobiles et une traçabilité des connexions.

- *Le recours aux prestataires*

Le recours à un prestataire dans le cadre de la mise en œuvre d'un traitement, y compris d'archives, est encadré par les dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

Ainsi, le responsable de traitement (ou son représentant) est tenu de prévoir un contrat écrit « *qui stipule notamment que le prestataire et les membres de son personnel n'agissent que sur la seule instruction du responsable de traitement ou de son représentant, et que les obligations visées aux deux premiers alinéas [dudit] article lui incombent également* ».

• *Les cas particulier du Cloud computing*

Le *Cloud computing* pourrait pleinement profiter des avantages de la 5G (vitesse élevée) et ouvrir une multitude de services, dont une sauvegarde qui s'enclenche automatiquement dès qu'il y a connexion.

Toutefois, eu égard aux risques inhérents au Cloud, il serait opportun de recommander le chiffrement, par le responsable de traitement, pour l'archivage des données dans le Cloud et de manière générale pour tout stockage de données, quel qu'il soit.

De même, il conviendrait de disposer d'une vision transparente des moyens réellement mis en œuvre par le prestataire (Cloud computing) afin d'assurer la sécurité et la sauvegarde des données qu'il héberge.

Force probante de la copie fiable et recevabilité des documents archivés de façon électronique : Les apports de la Loi n° 1.482 pour une Principauté Numérique

Alors que la destruction des archives physiques après leur numérisation n'était jusqu'à présent pas autorisée par la Loi, il convient de noter que le 27 décembre 2019, a été publiée au Journal de Monaco, la Loi n° 1.482 pour une Principauté Numérique qui s'inscrit dans le programme « *Extended Monaco* », visant à offrir un nouveau cycle de prospérité économique grâce aux outils numériques.

Ce texte qui modifie entre autres le régime probatoire de la copie en un texte unique (art. 1181) entraînant l'abrogation de l'art. 1182, al. 3 de l'art. 1184, al. 3 de l'art. 1195, prévoit que **la copie fiable a désormais la même force probante que l'original.**

Ainsi en vertu de l'article 15 de ladite Loi, « *La fiabilité est laissée à l'appréciation du juge. Est néanmoins réputée fiable la copie exécutoire ou authentique d'un écrit authentique. Est présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction du contenu du document dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par ordonnance souveraine. Lorsque les conditions de fiabilité de la copie sont réunies, conformément au précédent alinéa, la conservation de l'original n'est pas requise et sa destruction est autorisée dans des conditions fixées par ordonnance souveraine. Toutefois, si l'original subsiste, le juge pourra en demander la production* ».

Ces éléments autorisent donc implicitement la possibilité de détruire les originaux papiers, lorsque qu'ils sont numérisés et archivés électroniquement.

Par ailleurs, l'article 30-1 de cette même Loi ajoute un article 45 à la Loi n° 1.382 du 2 août 2011 sur l'économie numérique, modifiée, rédigé comme suit :

« *L'admission et la recevabilité d'un document archivé de façon électronique comme preuve en justice ne peuvent être refusées au seul motif que cet archivage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du service d'archivage électronique qualifié.*

Lorsqu'une obligation de conservation de données ou de documents est imposée par un texte légal ou réglementaire, cette obligation est présumée satisfaite par le recours à un service d'archivage électronique qualifié dont les exigences sont fixées par arrêté ministériel.

Sans préjudice de dispositions légales ou réglementaires particulières, les données électroniques conservées au moyen d'un service d'archivage électronique qualifié sont présumées avoir été conservées de manière à les préserver de toute modification ou altération nonobstant des modifications relatives à leur support ou leur format électronique ».

RECOMMANDATIONS À L'ATTENTION DES RESPONSABLES DE TRAITEMENT OFFRANT DES SERVICES EN LIGNE À DES ENFANTS

Cette fiche pratique concerne les services en ligne destinés aux enfants et a pour objet non seulement de mettre en lumière les principaux risques et enjeux pour la vie privée du jeune public liés à l'utilisation des services en ligne mais également de fournir des recommandations aux responsables de traitement offrant de tels services.

Elle a été réalisée sur la base du document de travail adopté en avril 2019 à Bled (Slovénie) par l'International Working Group on Data Protection in Telecommunication, dît Groupe de Berlin, dont la CCIN est membre.

Préambule

Parmi les utilisateurs des services en ligne, les enfants constituent une catégorie particulièrement vulnérable. Leur naïveté, et quelquefois leur incapacité à prendre des décisions éclairées, augmentent en effet chez eux le risque d'avoir le sentiment erroné de garder le contrôle de leurs données et d'adopter ainsi un comportement en ligne parfois dangereux. Dans certains cas, la collecte et l'utilisation des données personnelles concernant les enfants peuvent constituer des violations de la vie privée et de la protection des données. Elles peuvent également engendrer d'autres conséquences illégales, allant de la simple nuisance à des actes beaucoup plus graves, tels que le harcèlement sur internet ou l'exploitation sexuelle.

Les enfants passent beaucoup de temps à utiliser des services en ligne comme les sites internet, les applications, les services de jeu, les services vocaux ou encore les services de messagerie instantanée par le biais de nombreux appareils tels les smartphones, les tablettes, les PCs, les télévisions connectées et les assistants virtuels.

Ces services en ligne sont utilisés par les enfants pour une grande variété de raisons, que ce soit pour se divertir, interagir avec les amis, la famille et les tiers, écouter de la musique ou regarder des vidéos et rechercher des informations.

Tous ces services collectent et traitent des données personnelles, en commençant par les coordonnées, les données de localisation, les images fixes ou vidéo, les données d'utilisation ou encore les données d'interactions avec les services.

Les services en ligne doivent donc être protégés et conçus de manière adéquate afin de respecter les droits et la vie privée des personnes. Cela inclut, mais la liste n'est pas exhaustive, des mécanismes qui augmentent la transparence et assurent la validité du consentement donné pour la collecte et le traitement des données concernant les enfants.

Risques et facteurs aggravants

Les enfants sont en plein développement et n'ont pas encore les compétences requises pour agir en tant que citoyen numérique informé. Ils n'ont ainsi pas pleinement conscience des risques et dommages que peuvent engendrer la collecte et le traitement de leurs données personnelles. Les politiques de confidentialité sont difficiles à comprendre, même pour les adultes.

Les enfants n'ont pas toujours les connaissances requises pour gérer les paramètres de confidentialité et protéger leurs données personnelles.

Ils ne comprennent pas que la divulgation de données personnelles, y compris les coordonnées, peuvent entraîner le transfert de ces données à des tiers, ou l'intégration de ces données à d'autres sources de données disponibles, à leur insu. Il existe de nombreux risques que les données soient mal utilisées pour une variété d'objectifs comme la création de profils comportementaux, le vol d'identité, le harcèlement en ligne et même les abus sexuels.

Souvent, les applications et les sites internet partagent les données avec des tiers sans que les utilisateurs soient au courant. La complexité de ces systèmes et la technologie sous-jacente (cookies, iframes...) sont difficiles à appréhender par les adultes, et encore plus par les enfants.

La divulgation de données personnelles lors de l'utilisation de services en ligne a des conséquences à long terme, quelquefois irréversibles, pour le futur de l'enfant. Dans d'autres cas, les actions de l'enfant peuvent avoir un effet irréversible sur des personnes tierces (par exemple, en postant une photo ou un commentaire à propos de quelqu'un).

En raison des facteurs mentionnés ci-dessus, il n'est souvent pas possible d'obtenir des enfants un consentement éclairé en ce qui concerne la collecte et le traitement de leurs données lors de l'utilisation de services en ligne.

Bien que le consentement parental soit un outil effectif pour améliorer la protection de la vie privée et assurer le consentement éclairé à la collecte et au traitement des données, il nécessite, dans certains cas, des mécanismes d'authentification afin de déterminer l'âge de l'utilisateur et d'authentifier le consentement du parent/tuteur. La mise en place de tels mécanismes soulève le risque d'une collecte excessive de données, laquelle, à son tour peut constituer une violation de la vie privée.

Les principes

Les données personnelles des enfants ne doivent être collectées et traitées par les services en ligne **qu'après** avoir obtenu le consentement libre, explicite et éclairé de leurs parents/tuteurs, sauf lorsque :

a) l'enfant a atteint l'âge de consentement prévu par la Loi et a effectivement donné lui-même son consentement libre, explicite et éclairé ;

b) la collecte et le traitement des données sont basés sur un fondement juridique autre que le consentement (de la personne concernée ou de ses parents/tuteurs) ;

c) l'intérêt supérieur de l'enfant nécessite que les parents/tuteurs ne soient pas impliqués (par exemple, en cas de ligne directe mise en place pour la protection de l'enfance).

Les données des enfants doivent pouvoir être effacées à leur demande ou à celle de leurs parents/tuteurs afin de réduire toute conséquence négative pour l'avenir de l'enfant. En l'absence d'une justification raisonnable par exemple, une obligation légale de conserver les données, les responsables de traitement ne doivent pas refuser la demande d'effacement des données de l'enfant faite par celui-ci ou ses parents/tuteurs.

Les responsables de traitement ne doivent conserver les données des enfants que le temps nécessaire à la fourniture du service. Les adultes, dont les données personnelles ont été collectées et traitées alors qu'ils étaient enfants, doivent également avoir le droit de demander la suppression de ces données.

Le consentement parental

Soumettre la collecte et le traitement des données des enfants au consentement parental est un outil efficace pour surmonter la difficulté d'obtenir le consentement éclairé des enfants. Ainsi, lorsque le consentement est le fondement juridique du traitement, les responsables de traitement ne devraient traiter les données personnelles

des enfants **qu'après** avoir reçu le consentement des parents (sauf dans le cas d'une des trois exceptions énoncées précédemment dans le chapitre Principes).

Lorsque le service en ligne est offert au grand public et non uniquement aux enfants, mais qu'il est fréquemment utilisé par ces derniers, les responsables de traitement devraient faire des efforts raisonnables pour vérifier que l'utilisateur est un enfant et que le consentement est donné par les parents/tuteurs.

Les processus de vérification peuvent entraîner la collecte de données personnelles complémentaires sur les enfants et leurs parents/tuteurs. Les responsables de traitement et l'industrie au sens large sont donc encouragés à développer des mécanismes de vérification permettant de s'assurer de manière proportionnée de l'âge de l'utilisateur et de l'authenticité du consentement donné par les parents/tuteurs.

Dès que le responsable de traitement a connaissance que la personne concernée a atteint l'âge pour lequel l'accord parental n'est plus nécessaire, il ne doit pas se fonder sur le consentement donné par les parents/tuteurs pour continuer à conserver et utiliser des données collectées précédemment. Il doit au contraire obtenir le consentement de la personne concernée.

Transparence dans les services en ligne à destination des enfants

Les responsables de traitement doivent indiquer clairement aux enfants et à leurs parents/tuteurs que la fourniture des données est soumise à l'accord des parents/tuteurs (sauf si une obligation légale ou une autre base juridique applicable autorise la collecte des données sans l'accord desdits parents/tuteurs).

Les responsables de traitement doivent informer les enfants (si et dans quelles mesures les données sont collectées directement auprès d'eux) et les parents (sauf dans le cas d'une des trois exceptions énoncées précédemment dans le

chapitre Principes) notamment sur la collecte, l'utilisation et le traitement des données, la finalité pour laquelle les données sont collectées et les droits de l'utilisateur (droit d'accès par exemple) avant toute collecte de données.

Les responsables de traitement doivent détailler les catégories et le niveau de sensibilité des données collectées, les risques potentiels que les données soient transmises à des tiers et les coordonnées du responsable de traitement.

Les responsables de traitement doivent informer les enfants et leurs parents/tuteurs de leur droit à la vie privée, et de la manière dont les parents/tuteurs peuvent donner leur consentement à la collecte et au traitement des données de leurs enfants.

Cette information doit être donnée aux utilisateurs de manière accessible, claire et compréhensible en utilisant des moyens appropriés et adaptés aux enfants (dessins, vidéos, tableaux de bord...).

Mécanismes à intégrer dans les services en ligne pour enfants

Dès qu'ils prévoient une utilisation possible des services par des enfants, les responsables de traitement qui fournissent des services en ligne doivent penser à intégrer des mécanismes spécifiques à destination des enfants pour renforcer la sécurité de leurs données personnelles.

Les responsables de traitement devraient prévoir des mesures techniques et organisationnelles afin de s'assurer que, par défaut, seules les données personnelles nécessaires pour chaque finalité spécifique du traitement sont collectées, traitées et conservées. Cette obligation s'applique à la quantité de données collectées, à l'ampleur du traitement et à la durée de conservation.

Plus l'utilisateur du service en ligne est jeune, plus les mécanismes mis en place pour assurer la protection des données personnelles doivent être rigoureux.

Les catégories de données collectées et leur sensibilité doivent être également prises en considération lors de la mise en place de mécanismes permettant de renforcer la vie privée.

Les modifications des paramètres de confidentialité de nature à réduire la confidentialité des données ne devraient être possibles qu'après avoir obtenu l'accord des parents/tuteurs.

Le responsable de traitement doit expliquer aux enfants ainsi qu'aux parents/tuteurs l'importance des paramètres de confidentialité stricte et les mettre en garde contre les changements de ces paramètres, dans un langage clair et approprié pour l'âge, par le biais si nécessaire d'une aide visuelle. Cet avertissement doit apparaître dès que l'utilisateur demande à modifier les paramètres de confidentialité stricte pour des paramètres assouplis (par exemple, des paramètres qui impliquent des risques potentiels d'identification de l'enfant, la création des profils, l'installation des cookies).

Qualité des données

Les enfants grandissent et murissent au fil des années et en conséquence, les données les concernant deviennent souvent obsolètes et non pertinentes au regard des finalités pour lesquelles elles ont été à l'origine collectées et traitées.

Il est donc fortement recommandé de mettre en place des mécanismes qui permettent la correction, la mise à jour et l'effacement des données inexactes, non pertinentes ou excessives. Ces mécanismes doivent être adaptés à l'âge.

Droit d'accès

Les mécanismes pour le droit d'accès doivent être conçus de manière à répondre à l'intérêt supérieur de l'enfant, en tenant compte :

- des devoirs des parents/tuteurs pour le bien-être de l'enfant ;
- des droits de l'enfant à l'autonomie et à la vie privée ;
- de l'âge de l'enfant ou de la tranche d'âge à laquelle le service est destiné ;
- du type de service en ligne.

Commission de Contrôle des Informations Nominatives - 11ème Rapport d'Activité Annuel 2019

CCIN
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