PROTÉGER • INFORMER • PRÉVENIR

CCIN

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES



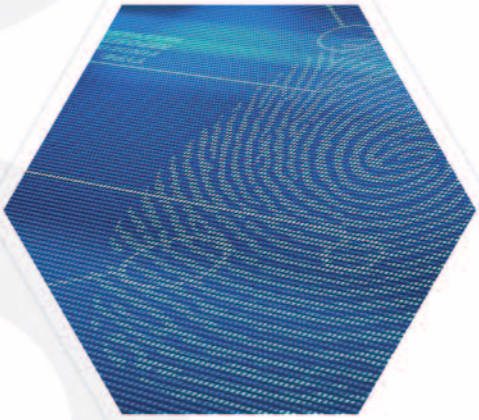




RAPPORT D'ACTIVITÉ 2018

10ème rapport public

ccin.mc



LE MESSAGE DU PRÉSIDENT

L'année 2018 a été marquée par le début des travaux menés conjointement entre les Services de l'Etat et de notre Commission, relatifs à la modification structurelle du droit interne régissant la protection des informations nominatives.

Cette refonte a pour vocation d'intégrer les modifications apportées à la Convention 108 telles qu'elles résultent du Protocole d'amendement adopté par le Comité des Ministres du Conseil de l'Europe au mois de mai 2018, et signé par les Autorités monégasques dès le 10 octobre 2018.

Elle s'attache également à prendre en compte les principes introduits sur le territoire de l'Union européenne par le Règlement Général sur la Protection des Données (RGPD), afin de faire bénéficier la Principauté des plus hauts standards en la matière.

Notre Commission se félicite vivement d'avoir été associée dès l'origine aux travaux préparatoires à l'élaboration du projet de loi destiné à remplacer la loi n° 1.165 relative à la protection des informations nominatives, qui devraient s'achever dans le courant de l'année 2019.

A cette occasion la CCIN a d'ores et déjà exprimé son souhait de faire bénéficier la future Autorité de protection des données d'une indépendance encore plus marquée, dans le strict respect du cadre constitutionnel et institutionnel de la Principauté, en ayant bien évidemment à l'esprit le Référentiel d'adéquation sur lequel la Commission européenne fondera son analyse lorsqu'elle aura à évaluer le niveau de protection des données personnelles garanti par la nouvelle législation monégasque, au regard du RGPD.

De plus cette évaluation s'effectuera également en prenant en compte la jurisprudence de la Cour de Justice de l'Union européenne relative aux garanties qui doivent être offertes par les pays tiers à l'Union européenne en matière d'accès et de traitements des données, par les Autorités publiques, à des fins de sécurité nationale.

Aussi la CCIN s'attachera à ce que la nouvelle législation monégasque réponde aux critères attendus par les Instances européennes.

En outre, les réflexions relatives à la modification prochaine du droit interne régissant la protection des données personnelles ont également été l'occasion pour notre Commission d'évoquer les modalités de fonctionnement et d'organisation de la future Autorité et de ses Services, à la lumière notamment des nouvelles missions qui seront les leurs.

L'entrée en application, le 25 mai 2018, du RGPD n'a pas été sans impacter de nombreuses entités situées à Monaco dont certains traitements de données personnelles entrent dans le champ d'application de ce nouveau texte.

Face aux interrogations relatives à la portée exacte du champ d'application du RGPD, le Comité européen de la protection des données a publié au mois de novembre 2018 des Lignes Directrices sur la portée extraterritoriale de ce Règlement, soumises à consultation publique.

La CCIN a participé à cette consultation publique afin d'évoquer, conjointement avec son homologue suisse, des points précis communs aux pays tiers à l'Union européenne mais dont la proximité géographique induit certaines problématiques spécifiques.

La version définitive de ces Lignes Directrices, dont la publication pourrait intervenir dans le courant de l'année 2019, devrait permettre utilement de déterminer avec davantage de précision le champ d'application territorial du RGPD.

Dans l'attente de ces précisions la CCIN a multiplié les réunions avec les entités de la Principauté potentiellement soumises au RGPD afin de les accompagner dans leur mise en conformité à ce nouveau texte européen, ainsi que dans l'accomplissement des formalités qu'elles ont à effectuer auprès de notre Commission au regard de la législation interne actuelle.

Plus que jamais, au cours de l'année écoulée nos actions se sont voulues empreintes de pédagogie et de dialogue afin de sensibiliser les responsables de traitements aux changements auxquels ils auront à faire face prochainement en Principauté, en s'inscrivant dans une démarche de « responsabilisation » et en mettant davantage encore la protection des données au cœur de leurs activités.

Pour autant notre Commission a également eu l'occasion d'affirmer son rôle de régulateur en charge du contrôle de la bonne application de la législation afin de défendre les droits et libertés des personnes concernées, dans un contexte où l'utilisation des données personnelles a parfois tendance à dévier de son objectif premier.

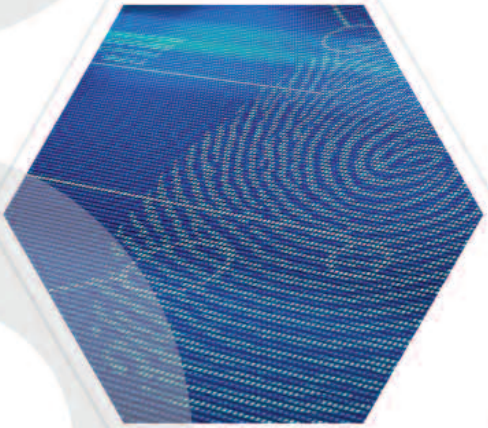
Guy MAGNAN

PROTÉGER • INFORMER • PRÉVENIR

RAPPORT D'ACTIVITÉ 2018

10ème 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.

En application de ces dispositions, les Commissaires ont été nommés par l'Ordonnance Souveraine n° 4.838 du 6 juin 2014.

De gauche à droite : Jean-Yves Peglion, Commissaire ; Rainier Boisson, Vice-Président ; Agnès Lepaulmier Stefanelli, Secrétaire Général ; Guy Magnan, Président ; Jean-Patrick Court, Commissaire ; 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.

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.

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.

Il assume de plus depuis le mois d'octobre 2018 la Présidence du Conseil pour le 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.

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 du Bureau d'assistance judiciaire ; de la Commission arbitrale des loyers ; de la formation correctionnelle statuant sur intérêts civils ; 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.

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 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, il apporte à la Commission son expérience diversifiée du fonctionnement des Institutions nationales et internationales acquise dans ses différentes fonctions.

Jean-Patrick COURT - Commissaire

Après avoir achevé un cursus universitaire de troisième cycle en droit et économie à l'Université de Paris I Panthéon Sorbonne, Jean-Patrick Court débute sa carrière professionnelle à la Banque de l'Union Européenne Paris en qualité d'économiste analyste financier puis d'attaché de direction.

En 1985 il intègre le Groupe Indosuez et prend la responsabilité de la zone Afrique et Amérique Latine de la BVCP. Trois ans plus tard il devient sous-directeur de la zone Europe du Crédit du Nord, puis Directeur Commercial de cet établissement à New-York.

En 1994 il revient en France pour prendre la Direction de l'Agence Centrale du Crédit du Nord de Lille-Rihour, puis il part en Angleterre durant une année où il est nommé Directeur Général du Crédit du Nord à Londres.

De 1998 à 2005 il assume successivement les fonctions de Directeur de la Division Industries et Grandes Entreprises du Crédit du Nord France puis de Directeur Délégué du Centre Grandes Entreprises de Paris.

Il prend ensuite la direction de la Banque Commerciale du Crédit du Nord de Monaco et depuis 2007 il est Directeur de Région de cet établissement et Directeur Général du Crédit du Nord de la Principauté.

Jean-Patrick Court est Membre de la Commission de Contrôle des Informations Nominatives depuis avril 2013, nommé sur proposition du Conseil Economique et Social, et fait largement bénéficier la Commission de sa longue expérience en matière bancaire et de sa maîtrise du fonctionnement des Places financières internationales.

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.

CCIN 1

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, lequel appréciera 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 un critère déterminant 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 2018 la Commission a disposé d'un budget global de 1.177.300,00 € se répartissant ainsi :

627.300,00 €
au titre des crédits de fonctionnement ;

550.000,00 €
au titre de ses dépenses salariales.

A l'occasion du Budget Primitif de l'exercice 2018 la Commission a bénéficié d'un crédit supplémentaire de 50.000,00 €, destiné à faciliter et à sécuriser les échanges avec les responsables de traitements par la mise à disposition d'outils numériques dédiés.

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.

L'ORGANISATION ET LES MISSIONS DU SECRÉTARIAT GÉNÉRAL

CCIN 2

Pour l'accomplissement de ses missions, la Commission est assistée d'un Secrétariat Général dont le fonctionnement et la coordination 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 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.

LA CCIN AUPRÈS DES INSTITUTIONS ET DES ACTEURS DE LA PRINCIPAUTÉ

CCIN 3

A l'occasion de la mise en place de l'échange automatique d'informations en matière fiscale la CCIN est intervenue lors d'une Conférence organisée au mois de février 2018 par le Département des Finances et de l'Economie, sous la Présidence de Monsieur Jean Castellini, Conseiller de Gouvernement-Ministre des Finances et de l'Economie. Cette présentation a permis à la CCIN de rappeler à l'ensemble des participants, représentant les Institutions bancaires et financières de la Place, leurs obligations déclaratives auprès d'elle s'agissant de la communication à la Direction des Services Fiscaux des informations de leurs clients soumis à ces obligations. Lors de cette Conférence les Services de l'Etat ont, de plus, présenté la plateforme dédiée à l'échange automatique d'informations en matière fiscale dont la mise en œuvre avait donné lieu à de nombreuses réunions préparatoires avec les Services de la Commission.

Dans le prolongement de l'entrée en vigueur de la Loi n° 1.430 portant diverses mesures relatives à la préservation de la sécurité nationale, les Agents de la CCIN ont participé à des réunions avec les représentants du Département de l'Intérieur et de la Direction de la Sûreté Publique afin d'évoquer les modalités de mise en œuvre des traitements désormais prévus par ce texte, et par ses Arrêtés Ministériels d'application. De nombreuses dispositions de la Loi n° 1.430 renvoyant à des textes réglementaires d'application, ces réunions ont été l'occasion d'évoquer avec les Services de l'Etat les éléments qui devaient figurer dans ces textes afin de répondre aux critères d'accessibilité et de prévisibilité pour les personnes concernées.

Dans le cadre des réflexions en cours relatives au développement des usages numériques en Principauté, la CCIN a été conviée à une présentation organisée par les Services Gouvernementaux et la Mairie portant sur la conception d'une plateforme « *M Road* » destinée à décliner les différentes fonctionnalités qui seraient offertes par le biais de la création d'une Identité Numérique en faveur, dans un premier temps, des nationaux et des résidents. Ce projet ambitieux a vocation à développer des e services dans de nombreux domaines, et se veut évolutif en fonction des besoins actuels et futurs.

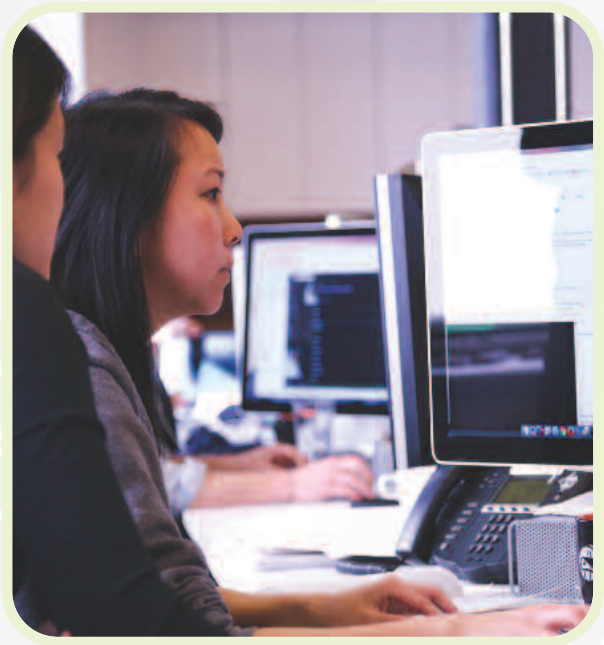
Compte tenu des différentes catégories de données qui seraient collectées et conservées, les points d'attention de la CCIN se sont tout naturellement portés sur les mesures de sécurité déployées, les accès dévolus par typologie de données, ainsi que leur durée de conservation. Des réunions thématiques ont également eu lieu sur la e-santé, ainsi que sur le développement d'outils mis à disposition des fonctionnaires et agents de l'Etat, et le projet de « *Smart City Monégasque* ». Ont également été évoqués le projet de création d'un « *cloud souverain* » et les mesures de sécurité qui devront y être associées.

Le traitement relatif à la gestion des passeports devant être mis à niveau afin de répondre aux standards actuels en la matière, des réunions avec le Secrétariat Général du Gouvernement ont été consacrées à la modification du traitement initial ayant fait l'objet d'un avis favorable de la Commission en 2003. L'objectif est d'intégrer aux actuels passeports un dispositif normalisé permettant de voyager plus facilement, et de veiller à l'intégrité des informations traitées.

Des réunions ont également eu lieu avec plusieurs Directions de l'Etat afin de les accompagner dans la mise à jour de leurs traitements. Tel a notamment

été le cas avec la Direction de l'Action et de l'Aide Sociales, soucieuse de réaliser une cartographie exhaustive de l'ensemble des données sensibles qu'elle traite (mesures à caractère social, données de santé, situations de handicap, ...). Il en a été de même avec la Direction de l'Environnement dans le cadre des actions menées auprès des entités publiques et privées mais également des particuliers à des fins de promotion des actions conduites par le Gouvernement Princier en matière de développement durable.

Au mois d'octobre la CCIN a assisté à une matinée d'information et de sensibilisation aux enjeux de la deuxième Evaluation Nationale des Risques (ENR) en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, organisée par le SICCFIN. A cette occasion, des agents du SICCFIN ont fait un compte rendu de la première ENR de la Principauté et des actions qui en ont découlé. Ils ont également attiré l'attention des participants sur la prochaine évaluation qui débutera en janvier 2019. Par ailleurs, un expert de la Banque Mondiale est intervenu afin de rappeler le fonctionnement de l'outil fourni par cette organisation, utilisé pour le premier exercice, et faire part de son analyse des résultats de cette première évaluation. Cette matinée a été clôturée par une intervention du Conseiller de Gouvernement – Ministre de l'Economie et des Finances qui a rappelé l'important travail réalisé par la Principauté de Monaco en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption (LAB-FT-C). Il a également invité les différents acteurs à faire le nécessaire afin que la Principauté conserve le niveau de conformité atteint et poursuive son développement social et économique dans le respect des plus hauts standards. Afin d'anticiper l'évolution de la législation régissant la matière le SICCFIN a souhaité rencontrer la CCIN en amont de l'exploitation de son nouvel outil métier qui aura vocation à recevoir de manière dématérialisée les déclarations de soupçon et à adresser des demandes de renseignements aux organismes assujettis à cette législation.



De plus dans le cadre des modifications législatives et réglementaires ayant pour objet d'intégrer en droit interne les dispositions de la Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015, communément appelée « *4ème Directive blanchiment* » la Commission de Législation du Conseil National a convié une délégation de la CCIN à prendre part à une réunion de travail afin d'évoquer les modifications qui seraient apportées à la Loi n° 1.362 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption. Ont ainsi été notamment évoquées la création d'un registre des Bénéficiaires Effectifs, l'introduction d'un droit d'accès indirect aux informations détenues par les entités assujetties exercé par la CCIN à la demande des personnes concernées, ainsi que la problématique des durées de conservation des

informations traitées en matière de LAB-FT-C. Ces échanges ont permis d'aborder également l'extension du champ des éléments faisant l'objet d'une déclaration au SICCFIN, ainsi que la notion de « *sources fiables* » devant être utilisées par les entités assujetties aux fins de procéder aux vérifications de leurs clients ou prospects dans le cadre de l'évaluation des risques en matière de LAB-FT-C.

L'année 2018 a également été mise à profit pour initier la réflexion menée conjointement avec les Services de l'Etat relative à la modification du droit interne régissant la protection des informations nominatives, afin d'y introduire les principes découlant du Règlement Général sur la Protection des Données (RGPD). L'objectif de cette refonte est triple :

- uniformiser les obligations des responsables de traitements en Principauté de Monaco et sur le territoire de l'Union européenne afin de rationaliser les processus de conformité ;
- conférer aux personnes concernées les mêmes standards de préservation de leurs droits ;
- relancer la procédure de reconnaissance du niveau de protection adéquat de la législation monégasque dont l'évaluation se fera désormais à l'aune du RGPD.

Tout en ayant à l'esprit la nécessité d'intégrer à Monaco les principes de cette nouvelle régulation européenne, le Gouvernement et la Commission ont à cœur de prendre en considération les spécificités du fonctionnement institutionnel et du tissu économique de la Principauté. Les discussions ont également porté sur les modalités d'introduction en droit interne de la Directive 2016/680 du 27 avril 2016 communément appelée « *Directive Police-Justice* ».

Au cours de l'année écoulée la Commission a poursuivi ses réunions périodiques avec l'Association Monégasque des Activités Financières (AMAF) dont la plupart des Membres a été impactée dès le 25 mai 2018 par l'application du RGPD. Les principales questions ont concerné les contours de son champ d'application extraterritorial et des obligations qui en découlent pour les entités de la Principauté qui y sont soumises, dont notamment la désignation d'un représentant sur le territoire de l'Union européenne et d'un Délégué à la Protection des Données, la poursuite de l'application de la Loi n° 1.165 sur la protection des informations nominatives et son articulation avec le RGPD. La modification de la Loi n° 1.362 relative à la LAB-FT-C intervenue en juin 2018 a également donné lieu à des échanges portant sur les communications au sein d'un même Groupe des informations traitées en la matière, ainsi que sur les durées de conservation des données.

Par ailleurs de nombreuses entités bancaires et financières ont souhaité rencontrer les Services de la Commission afin d'évoquer leurs situations spécifiques dans un contexte global de rationalisation des fonctions supports et des coûts associés.

Le Secrétariat Général de la Commission a été convié à participer à une réunion du Comité de Direction de Monaco Télécom au cours de laquelle ont été évoquées les obligations pesant sur cette société pour ses activités désormais soumises au RGPD, et également sur les contraintes liées à sa qualité d'opérateur de réseaux et de services de télécommunications et de communications électroniques.

Une réunion de présentation a été organisée en collaboration avec Monacotech afin de sensibiliser les responsables des startups à leurs obligations en matière de protection des données personnelles dans des domaines aussi variés que le yachting, la gestion de patrimoine, le développement durable ou encore les implants médicaux.

Le 10 juillet, plusieurs agents du Secrétariat Général se sont rendus, à l'invitation de l'Association des Industries Hôtelières Monégasques (A.I.H.M), au Fairmont Monte-Carlo, pour présenter aux membres de cette association les obligations qui leur incombent en vertu de la Loi n°1.165 en matière de protection des données. La CCIN a notamment mis l'accent sur les dispositifs de vidéosurveillance, en rappelant que dans les restaurants et bars, les caméras peuvent filmer les portes d'entrée et de sorties, les zones de stockage, les réserves, les caves et le parking intérieur, extérieur et/ou souterrain, mais qu'en revanche lesdites caméras ne peuvent pas filmer les clients lorsqu'ils sont à table ou installés au comptoir, ni les employés dans leurs zones de travail, sauf justification particulière (par exemple : les caisses). Concernant les hôtels, elle a rappelé qu'un dispositif de vidéosurveillance peut être installé au niveau des entrées et sorties des bâtiments, au niveau des issues de secours, aux abords de la piscine et peut être utilisé dans les couloirs mais uniquement lors d'une situation de crise ou d'urgence pour prévenir un risque de panique lors d'une évacuation ou lors d'un litige avec un client dans le cadre d'une infraction.

Le milieu associatif et caritatif étant particulièrement dynamique en Principauté, de nombreuses réunions ont été organisées en 2018 à des fins d'accompagnement à la mise en conformité et de sensibilisation à la protection des données personnelles.

Ainsi, les représentants de la Croix Rouge Monégasque ont pris l'attache de la Commission afin de mettre à jour leurs formalités en tenant compte de l'évolution de leurs nombreuses missions.

Créée en 2014 dans le cadre de la Loi n° 1.384 du 20 juillet 2011 relative à la prévention et à la répression des violences particulières, l'Association d'Aide aux Victimes d'Infractions Pénales (AVIP) accueille les victimes, les informe sur leurs droits et met à leur disposition un accompagnement juridique, social et psychologique personnalisé. Compte tenu de l'extrême sensibilité des informations dont elle a à

connaître, l'AVIP est particulièrement soucieuse de la confidentialité des données relatives aux victimes qu'elle prend en charge. C'est dans ce contexte que des réunions ont été organisées afin de l'assister dans la sécurisation de son système d'information.

En partenariat avec Action Innocence Monaco, des agents du Secrétariat ont animé, le 13 novembre 2018, une session de prévention destinée à informer et sensibiliser les parents d'élèves sur les risques et dérives liés à l'utilisation des réseaux sociaux. Ces outils sont en effet devenus indispensables aux enfants et aux adolescents puisqu'ils communiquent désormais essentiellement via Snapchat ou WhatsApp, échangent des photographies et téléchargent des vidéos ou des musiques, sans nécessairement avoir conscience de la manne de données personnelles qu'ils partagent avec la terre entière. Organisé à la Casa d'i Soci, cet échange a donc été l'occasion pour la CCIN de partager son expérience et son expertise en la matière et de promouvoir une pratique sécurisée d'Internet, en proposant des réflexes à adopter et des solutions pratiques à mettre en place.

Dans le cadre de ses missions de sensibilisation la CCIN a effectué une campagne d'affichage sur les panneaux municipaux afin de sensibiliser les particuliers et les professionnels à la protection des informations nominatives. Cet affichage a été réalisé à l'occasion de la 12ème Journée européenne de la Protection des Données Personnelles. Créée en 2007 par le Conseil de l'Europe et relayée par la Commission européenne, la « *Journée européenne de la protection des données à caractère personnel* » a, comme son nom l'indique, pour objectif principal de sensibiliser les personnes sur l'importance de la protection de leurs informations nominatives. Elle est célébrée le 28 janvier de chaque année. Ce jour n'a d'ailleurs 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.

L'affiche réalisée à cette occasion mentionne divers domaines dans lesquels des informations nominatives pouvaient être traitées (vidéosurveillance, publicité, profilage, réseaux sociaux, données de santé, documents d'identité, etc.) et rappelle aux particuliers et aux professionnels l'existence de droits et responsabilités en matière de protection des données personnelles.

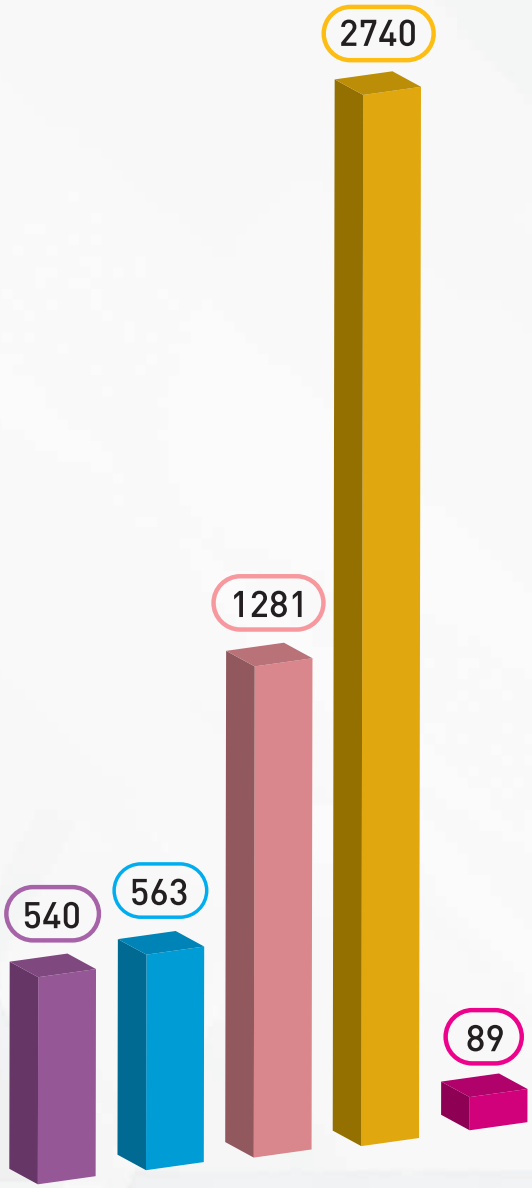
LE RÉPERTOIRE PUBLIC DES TRAITEMENTS

CCIN 4

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 2018

5.213 se répartissant ainsi :

- 540 Traitements du secteur public ou assimilé
- 563 Traitements ayant fait l'objet d'une autorisation de la Commission
- 1281 Traitements ayant fait l'objet d'une déclaration ordinaire
- 2740 Traitements ayant fait l'objet d'une déclaration simplifiée
- 89 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
DS		26	26	68	21	16	45	46	19	54	856	144	86	180	201	162	221	243	326
DO	5	20	20	75	51	60	55	82	42	56	51	32	79	55	121	115	81	140	141
DA	6	22	22	13	17	11	2	12	16	4	22	38	71	68	67	23	34	38	54
DAUT								1		1	7	38	38	31	87	62	89	119	90
TRANSFERT														1	1	4	21	21	41

Nombre de nouveaux traitements inscrits au répertoire en 2018 :

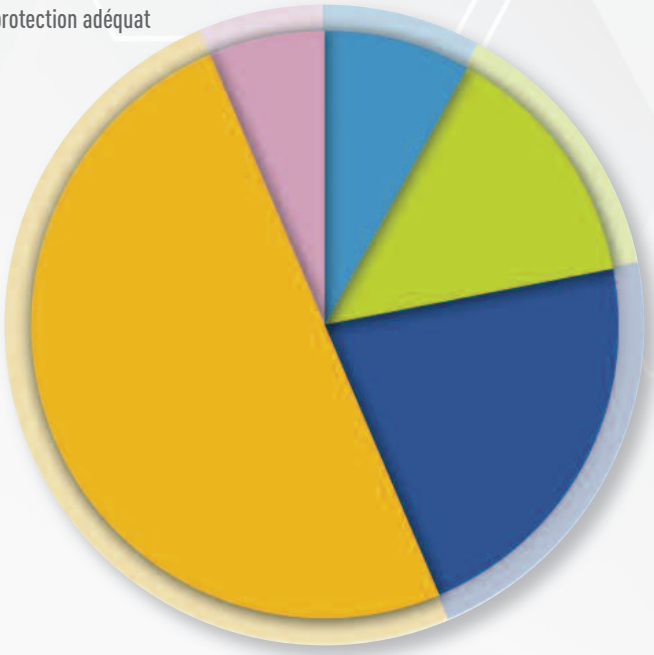
652 traitements ont été inscrits au répertoire public, se répartissant comme suit :

41

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

54

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



90

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

326

traitements ayant fait l'objet d'une déclaration simplifiée

141

traitements ayant fait l'objet d'une déclaration ordinaire

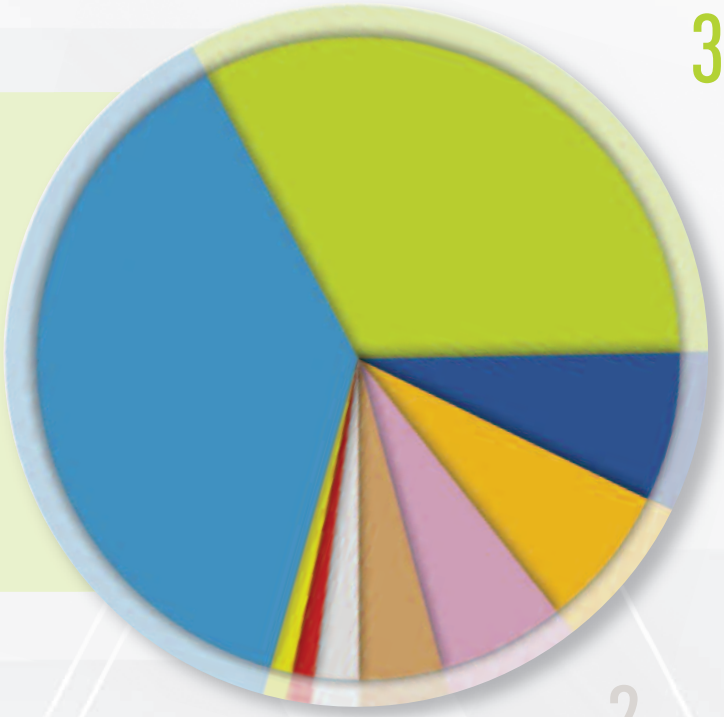
L'accroissement sensible du nombre d'autorisations de transfert depuis 2 ans s'explique par le fait qu'au mois d'avril 2015 la Commission a arrêté une position de principe aux termes de laquelle les transferts d'informations nominatives vers un Pays ou un organisme n'assurant pas un niveau de protection adéquat doivent, en toutes hypothèses, lui être soumis en la forme d'une demande d'autorisation de transfert, indépendamment du fait qu'ils relèvent de l'alinéa 1er ou 2ème de l'article 20-1 de la Loi n° 1.165, modifiée.

Il est à noter qu'un accès à un traitement donné à une entité située dans un Pays ne disposant pas d'un niveau de protection adéquat est analysé en un transfert d'informations nominatives et nécessite de ce fait l'autorisation préalable de la Commission.

Nombre de délibérations rendues par la Commission en 2018 :

Au cours de l'année écoulée, la Commission a rendu 210 délibérations se répartissant ainsi :

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



36 autorisations relatives à des dispositifs de vidéosurveillance

31 autorisations relatives aux traitements concernant plus spécifiquement le secteur bancaire et assimilé

7 autorisations relatives aux enregistrements téléphoniques

7 autorisations relatives à la gestion des contentieux

6 autorisations relatives à des dispositifs de contrôle d'accès biométriques ou non

4 autorisations relatives à la messagerie électronique

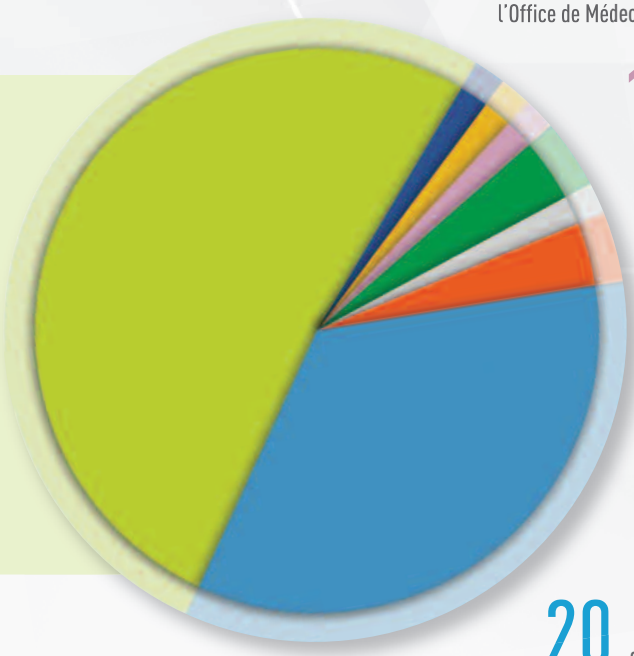
2 autorisations relatives aux obligations spécifiques en matière de vérifications des sportifs de haut niveau

1 autorisation relative aux alertes professionnelles

1 autorisation relative à un traitement de géolocalisation

3 portant refus d'autorisation

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



1 demande d'avis présentée par la Commune

1 demande d'avis présentée par l'Office de Médecine du Travail

1 demande d'avis présentée par la SMEG

2 demandes d'avis présentées par la Compagnie des Autobus de Monaco

1 demande d'avis présentée par l'Office de la Médecine du Travail

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

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

30 demandes d'avis présentées par le CHPG

41 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 ;

9 Portant avis sur des projets de textes transmis par le Ministre d'Etat ;

2 Portant fixation de délais de conservation plus brefs que ceux souhaités par les responsables de traitements ;

2 Portant sur une mission d'investigation.

CCIN 5

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 2018 ce répertoire a été consulté 12 fois :

- Cinq fois par des salariés dont à 3 reprises par les Délégués du Personnel. Ces consultations ont concerné :
  - un traitement relatif à la gestion des ressources humaines ;
  - quatre dispositifs de vidéosurveillance.
- Six fois par des professionnels :
  - une fois par un Avocat pour le compte de son client afin de vérifier si le dispositif de décompte des heures de travail mis en œuvre par l'employeur de son client avait fait l'objet de formalité auprès de la CCIN ;

  - une fois par un Cabinet d'Expert-Comptable afin de vérifier la conformité de 3 de ses clients à la législation relative à la protection des données personnelles ;
  - quatre fois par des responsables d'entités afin de faire le point sur les formalités déjà effectuées, dans la perspective de régulariser leur situation.
- Une fois par un membre d'une association qui souhaitait obtenir la liste de tous les autres membres de ladite association afin de les contacter. Cette consultation du répertoire public des traitements a permis de préciser que la CCIN ne détient aucune liste d'informations nominatives contenues dans les traitements qui lui sont soumis (ex : liste du personnel, des clients, ...) et d'indiquer à la personne que les catégories de destinataires des listes des membres des associations sont régies par l'Arrêté Ministériel n° 2010-195 du 7 avril 2010 relatif aux modalités de déclaration simplifiée de conformité des traitements automatisés d'informations nominatives portant sur la gestion des membres des associations ou des fédérations d'associations.

Bien souvent lorsque la consultation du répertoire fait apparaître l'exploitation illicite d'un traitement automatisé d'informations nominatives une plainte est déposée auprès du Président de la Commission. Ainsi en 2018 trois plaintes ont fait suite à une consultation du répertoire public des traitements.

LES PLAINTES

15 plaintes ont été adressées à la Commission en 2018, en légère augmentation par rapport à l'année précédente au cours de laquelle la CCIN avait été saisie par 13 plaignants.

La défense des droits des personnes concernées

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.

4 plaintes ont été reçues en 2018 concernant le droit de suppression.

Le « *droit à l'oubli* »

Dans le prolongement de la décision communément appelée « *Google Spain* » du 13 mai 2014 de la Cour de Justice de l'Union Européenne, la CCIN a été saisie de 4 demandes de déréférencement ou de suppression de faux profils ou de propos diffamatoires auprès du moteur de recherche Google, mais également auprès de Facebook et deTwitter.

La première plainte a concerné la demande de suppression d'un faux profil Twitter et a fait suite à une première plainte reçue en 2017 concernant le retrait de faux profils Facebook, Linkedin, Twitter et Youtube créés en vue de nouer des relations d'affaires en se faisant passer pour le dirigeant d'un établissement bancaire de la Principauté, et pour son assistante.

En effet, suite à la suppression obtenue en 2017 le faux profil de l'assistante du dirigeant créé sur Twitter était de nouveau accessible.

Une nouvelle intervention de la CCIN a permis d'obtenir rapidement la suppression de ce profil.

La deuxième plainte a elle aussi fait suite à un déréférencement obtenu précédemment mais pour lequel il est apparu que l'article portant préjudice au plaignant était à nouveau accessible depuis une connexion internet de Monaco.

Suite à une nouvelle intervention de la CCIN auprès de Google, et après avoir identifié précisément l'URL concernée en vérifiant notamment la casse et la ponctuation, l'article préjudiciable n'est à nouveau plus accessible, y compris depuis Monaco.

Lorsque des faux profils ou propos sont supprimés d'une plateforme ou d'un moteur de recherche il peut arriver qu'ils soient à nouveau accessibles après un certain temps.

Aussi il est important que les personnes concernées vérifient régulièrement que les contenus inopportuns ne sont pas à nouveau en ligne.

Dans la troisième plainte il s'agissait d'un membre d'une profession réglementée dont une des clientes avait publié sur son compte Facebook accessible par plus de 900 personnes, dont nombre se trouvent en Principauté, des propos insultants portant atteinte à la réputation du plaignant.

Celui-ci n'ayant pas pu obtenir de Facebook la suppression des propos en cause, il a saisi la CCIN afin qu'elle intervienne auprès de cette plateforme.

Même si au moment de l'intervention de la Commission les propos semblaient avoir été supprimés, il a été demandé confirmation à Facebook de cette suppression.

A cette occasion il a été rappelé que tout utilisateur de ce réseau social peut directement alerter ses administrateurs sur un contenu, un commentaire ou une photo par le biais de la fonction « *Signaler* ».

Toutefois en cas de difficulté la saisine d'une Autorité de protection des données permet d'obtenir rapidement la suppression de propos diffamatoires ou de faux profils.

Enfin dans la quatrième plainte la CCIN a été saisie par un restaurateur suite à la publication de commentaires extrêmement défavorables d'une cliente par le biais d'une publication sur le mur public de son compte Facebook, et du dépôt d'un avis de restauration sur Google.

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* ».

Au cas d'espèce il a été pris acte que l'Avocat du restaurateur avait attrait, par voie de citation directe, l'auteur de ces propos en justice afin de répondre du délit de diffamation publique, et qu'il incombait aux Autorités judiciaires d'apprécier cette qualification, et le cas échéant d'obtenir la suppression des commentaires en cause.

Par ailleurs au cours de l'année écoulée 4 plaintes ont concerné le droit d'accès aux informations.

Le droit d'accès

Conformément à l'article 13 de la Loi n° 1.165 toute personne physique a le droit d'accéder aux informations la concernant et d'obtenir qu'elles soient modifiées s'il y a lieu, l'article 15 venant pour sa part préciser que la réponse à une demande d'accès doit s'effectuer sous un délai d'un mois.
En application de ces dispositions deux plaignants ont saisi la Commission en 2018.

Dans le premier cas il s'agissait d'une personne ayant fait l'objet d'une mesure de consigne de la part d'un établissement de jeux de la Principauté, qui souhaitait connaître les motifs ainsi que les justifications de cette mesure.

Dans le cadre de l'instruction de ce dossier il a cependant été constaté que le courrier adressé audit établissement ne mentionnait pas de manière explicite la demande d'obtenir communication des informations relatives à l'intéressé. Aussi le plaignant a été invité à reformuler sa demande de droit d'accès de manière précise, en justifiant de son identité conformément à l'article 15 de la Loi n° 1.165.

S'agissant de la justification de la mesure de consigne dont il a fait l'objet la CCIN lui a rappelé les termes de la Loi n° 1.103 du 12 juin 1987 relative aux jeux de hasard exploités en Principauté, et plus particulièrement de son article 10, lequel dispose que :

« *Sont exclus des maisons de jeux selon des modalités fixées par ordonnance souveraine :*

1° les personnes qui en font la demande par écrit ;

2° les incapables sur la demande écrite de leur représentant légal ou de leur curateur ;

3° les personnes qui seront jugées indésirables.

Les exclusions prononcées pour une durée supérieure à un an ne prennent effet qu'après agrément administratif.

L'autorité administrative peut toujours prescrire l'exclusion d'une personne déterminée. »

A cette occasion le plaignant, qui considérait avoir fait l'objet d'un fichage illicite et arbitraire, a été informé que le traitement relatif à la gestion des consignés était légalement mis en œuvre au sens de la législation relative à la protection des informations nominatives.

La seconde plainte a concerné une difficulté d'accès aux données relatives à une mesure d'interdiction bancaire auprès d'un établissement monégasque.

En dépit de 2 demandes effectuées par l'Avocat des plaignants auprès de l'établissement concerné aucune information n'avait été communiquée.

A l'issue de l'intervention du Président de la CCIN l'établissement a finalement répondu aux plaignants concernant la mesure d'interdiction bancaire en question.

Par ailleurs la Commission a été saisie d'une demande d'accès aux informations nominatives d'une personne décédée.

Les modalités d'accès à ces informations sont également régies par l'article 13 de la Loi n° 1.165 :

« *Sauf dispositions législatives contraires, l'ascendant, le descendant jusqu'au second degré, ou le conjoint survivant d'une personne décédée, peut, s'il justifie d'un intérêt, exercer les droits prévus au précédent alinéa [droit d'accéder aux informations et d'en obtenir modification s'il y a lieu], pour ce qui est des informations concernant cette personne* ».

L'objet de cette saisine concernait l'accès, par la fille du défunt, aux informations détenues par un établissement bancaire sur son père.

En effet après une demande effectuée directement par la plaignante auprès de l'établissement bancaire, l'intéressée n'avait pas reçu l'intégralité des informations souhaitées, dont certaines concernaient les années 2002 à 2004.

Sur ce point, après avoir rappelé les conditions légales d'accès aux informations des personnes décédées, la Commission a également précisé à la plaignante les principales durées de conservation des informations détenues par les établissements bancaires, dont notamment :

- dans le cadre des traitements relatifs à la « *Tenue des comptes de la clientèle* », l'article 4 de l'Arrêté Ministériel n° 2002-270 du 23 avril 2002 prévoit une durée de conservation des informations de 10 ans maximum ;

- dans le cadre des traitements relatifs aux « *Valeurs mobilières et autres instruments financiers* », l'article 4 de l'Arrêté Ministériel n° 2002-269 du 23 avril 2002 prévoit une durée de conservation des informations de 10 ans maximum ;

- dans le cadre des traitements relatifs à la « *gestion des crédits et prêts consentis à des personnes physiques* », l'article 4 de l'Arrêté Ministériel n° 2002-268 du 23 avril 2002 prévoit que les informations ne peuvent être conservées au-delà de la durée d'exécution du contrat pour lequel lesdites informations ont été collectées.

Ces délais de conservation relatifs aux traitements les plus usuels exploités par les banques ayant été rappelés à la plaignante, la Commission l'a invitée à se rapprocher de l'établissement afin

de se faire confirmer que les informations souhaitées n'avaient pu lui être communiquées car elles avaient été supprimées.

Enfin, la quatrième plainte relative à l'accès aux informations concernait également des informations détenues par un établissement bancaire.

Dans ce cas toutefois la plaignante avait déjà reçu les informations la concernant de la part de l'établissement, mais elle souhaitait avoir également communication des informations relatives aux sociétés patrimoniales et fondations dont elle est membre, actionnaire, sociétaire ou ayant droit.

Aussi il lui a été précisé que si l'article 13 de la Loi n° 1.165 consacre un droit d'accès, par les personnes morales aux informations les concer-

nant [« *Toute personne morale a le droit d'accéder (...) aux informations la concernant* (...)], il n'en demeure pas moins que cet accès ne peut être effectué qu'au bénéfice des représentants légaux de ces entités. A défaut l'établissement bancaire sollicité pourrait enfreindre l'article 308 du Code pénal relatif au secret professionnel.

L'exploitation des traitements automatisés d'informations nominatives

Au cours de l'année écoulée 7 plaintes ont été adressées à la Commission relatives à la conformité des traitements et à la licéité de la collecte et de l'exploitation des données personnelles.

La conformité des traitements

Conformément à la législation monégasque, tous les traitements automatisés d'informations nominatives sont soumis à l'accomplissement de formalités auprès de la CCIN préalablement à leur mise en œuvre, sauf le cas où un Arrêté Ministériel les dispense, sous conditions, de l'accomplissement de formalités. Il est à noter qu'à ce jour seuls sont dispensés de formalité préalable les traitements automatisés relatifs à la gestion de la paie des personnels, sous réserve de respecter les dispositions de l'Arrêté Ministériel n° 2016-502 du 5 août 2016 fixant les modalités de cette dispense.

Dans ce cadre la question de la conformité de la mise en œuvre des traitements automatisés d'informations nominatives au regard des dispositions régissant la protection des données a été à l'origine de 4 plaintes en 2018, dont 3 ont fait suite à une consultation du répertoire public des traitements au siège de la Commission.

La première plainte concernait un dispositif de dépose de curriculum vitae et de tests d'embauche en ligne, non légalement mis en œuvre car n'ayant jamais été soumis à la CCIN. L'intervention du Président de la Commission a permis de suspendre sur le champ l'exploitation de ce traitement, dans l'attente de sa régularisation.

Dans le second cas il s'agissait également d'un outil informatique, mis cette fois à la disposition de certains employés afin de réaliser des tests de personnalités. Après instruction de ce dossier il est apparu que l'employeur avait souhaité mettre à disposition ces tests dans le but que les salariés concernés puissent appréhender leurs besoins en formations afin de pouvoir approfondir leurs aspirations en matière de formation professionnelle. Il a de plus été pris acte du fait que ni l'employeur, ni les supérieurs hiérarchiques des personnes qui réaliseraient ces tests n'auraient connaissance des résultats.

Les deux autres plaintes ont concerné des dispositifs de vidéosurveillance exploités sur le lieu de travail et pour lesquels aucune autorisation de mise en œuvre n'avait été délivrée par la Commission.

Dans les deux cas la Commission a été saisie par des salariés et, compte tenu des éléments qui ont été portés à sa connaissance lors de sa saisine, elle a décidé de mener une mission de contrôle dans les établissements concernés afin de vérifier l'existence d'un tel dispositif ainsi que les modalités de son exploitation et l'utilisation qui en était faite par l'employeur.

En effet la Commission se montre extrêmement attentive à la multiplication des systèmes de caméras sur le lieu de travail et veille à ce que ces dispositifs ne permettent pas de contrôler le travail ni le temps de travail des salariés, et ne soient pas détournés de leur finalité première qui consiste à assurer la protection des personnes et des biens.

La licéité de la collecte et de l'exploitation des informations

L'article 10-1 de la Loi n° 1.165 dispose que les informations nominatives doivent être collectées et traitées loyalement et licitement.

Sur ce fondement 3 plaintes ont été adressées à la Commission en 2018.

La première a concerné le dispositif de gestion des courses de taxi, dont la mise en œuvre avait fait l'objet d'un avis favorable de la Commission par délibération n° 2018-042 du 21 mars 2018.

Cependant la plainte mentionnait que le numéro attribué à chaque taxi de la Principauté apparaissait dans l'applicatif de gestion mis à la disposition de chaque conducteur, leur permettant ainsi de savoir en temps réel à quelle station se trouvaient leurs collègues, désignés par leur numéro de taxi, ainsi que la durée de leur présence à ladite station, de même que le statut de leur véhicule (libre, en charge, à destination, indisponible).

Si la délibération susmentionnée avait pris acte de la fonctionnalité de géolocalisation des taxis en service afin d'optimiser le service rendu aux clients, il n'était pas fait mention du fait que tous les conducteurs connaissaient la position en station ainsi que le statut de l'ensemble des taxis de la Principauté.

Aussi il a été demandé au responsable de traitement de désactiver cette fonctionnalité qui faisait apparaitre des informations nominatives en ce qu'elle permettait à chaque conducteur de taxi de connaître la position en station ainsi que le statut de tous les autres conducteurs.

Il lui a de plus été précisé que s'il était envisagé d'implémenter légalement cette fonctionnalité nominative il importait alors de soumettre à la Commission une demande d'avis modificative relative au traitement ayant pour finalité la « *Gestion du service des courses de taxi* » en justifiant de l'intérêt et de la proportionnalité qui s'attachent, pour les conducteurs de taxi, à avoir connaissance en temps réel, du statut et de l'emplacement en station des autres conducteurs.

En réponse à la démarche du Président de la Commission il a été indiqué que l'application allait être modifiée afin de ne plus faire apparaitre les numéros des taxis, mis à part pour les conducteurs qui auront formellement donné leur accord pour que leur numéro soit visible dans l'application.

Dans la deuxième plainte reçue en fin d'année 2018 il s'agissait d'un dispositif de vidéosurveillance dont la mise en œuvre avait fait l'objet d'une autorisation par la Commission.

Toutefois, lors d'une consultation du répertoire public des traitements, des salariés de l'établissement ont constaté que l'autorisation ne concernait pas la possibilité, pour la Direction, d'accéder à distance aux images issues des caméras de vidéosurveillance, et ont indiqué que certains éléments les conduisaient à penser que la Direction disposait d'accès distants.

S'agissant d'accès distants aux images de vidéosurveillance la Commission tient à s'assurer qu'ils soient sécurisés afin de ne pas permettre à des tiers non autorisés de visualiser les images.

De plus lorsque ces accès distants sont ouverts à des membres de la Direction, la CCIN veille à ce que les salariés en soient explicitement informés, et elle rappelle systématiquement que les dispositifs de vidéosurveillance ne doivent pas être utilisés à des fins disciplinaires autres qu'en cas d'atteinte à la sécurité des personnes ou des biens.

Afin de vérifier l'existence de ces accès distants, et l'éventuelle utilisation qui serait faite des images de vidéosurveillance, la Commission a souhaité qu'un contrôle de ce dispositif soit effectué en 2019.

Par ailleurs, en fin d'année 2017 la Commission avait été saisie d'une plainte relative à l'exploitation d'une messagerie électronique qui n'avait fait l'objet d'aucune formalité, et pour laquelle la régularisation est intervenue en début d'année 2018, suite à l'intervention du Président de la CCIN.

Toutefois, dans le prolongement de cette plainte initiale, il a été indiqué à la CCIN que l'ancien employeur du plaignant aurait accédé, en 2015, à des emails personnels du plaignant. Sur ce point, les éléments qui ont été portés à la connaissance de la Commission ne permettaient pas de vérifier si, effectivement, les messages concernés étaient soit des messages privés, soit des messages issus de la messagerie personnelle du plaignant, accessible depuis l'ordinateur portable professionnel mis à sa disposition par son employeur.

De plus, il a été pris acte du fait que l'ensemble des éléments et documents en cause, dont la CCIN n'a pas eu connaissance, avaient été produits en justice dans le cadre de procédures pénales en cours, et que de ce fait il appartenait au Tribunal de Première Instance de se prononcer sur une éventuelle violation de la vie privée du plaignant, au regard des pièces du dossier.

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 doivent être signalées au Procureur Général, le Président de la Commission avait, courant 2014, transmis au Parquet une plainte concernant la licéité de l'exploitation de données de géo positionnement, ainsi qu'un refus de réponse à une demande de droit d'accès.

Dans le cade de l'instruction de ce dossier le Parquet a souhaité obtenir des précisions complémentaires, ainsi que les observations du Président de la CCIN sur les derniers éléments du dossier.

Par ailleurs en 2015 la CCIN avait été saisie d'une plainte portant sur les difficultés que rencontrait un patient à obtenir communication de son dossier médical. De nombreux échanges avec l'intéressé ainsi qu'avec les représentants du responsable de traitement avaient permis de faire le point sur l'ensemble des éléments dont la communication était demandée, et l'établissement avait transmis à la personne concernée les documents dont il disposait.

Le Procureur Général, saisi d'une plainte par le patient, a souhaité que le Secrétaire Général de la CCIN soit entendu au cours de l'année 2018 par un Officier de Police Judiciaire.

LES SANCTIONS

En application de l'article 19 de la Loi n° 1.165, le Président de la Commission a adressé en 2018 un avertissement, qui a donné lieu à publication sur le site Internet de la CCIN ainsi qu'au Journal de Monaco.

Cet avertissement a fait suite à un contrôle effectué en fin d'année 2017 portant sur le dispositif de vidéosurveillance exploité au sein du Café de Paris par la Société des Bains de Mer et du Cercle des Etrangers (SBM).

Les irrégularités relevées lors de ce contrôle étaient nombreuses :

- exploitation d'un dispositif de vidéosurveillance antérieure à l'autorisation de la CCIN ;
- défaut de maîtrise des durées de conservation des données ainsi que des habilitations d'accès aux images ;
- implantation de caméras filmant les salariés à leur poste de travail ainsi que les clients attablés en terrasse ;
- non-respect de l'obligation d'information des personnes concernées ;
- inexistence de clauses contractuelles avec le prestataire technique relatives à ses obligations en matière de préservation de l'intégrité des informations nominatives.

Il a de plus été constaté que, contrairement à ce qu'avait indiqué un Membre de la Direction de la SBM au Président et au Secrétaire Général de la CCIN quelques mois avant le contrôle, aucune caméra du Café de Paris n'avait été désactivée suite à une première intervention de la Commission auprès de cet établissement.

L'ensemble de ces éléments a conduit le Président de la CCIN à publier cet avertissement, conformément au dernier alinéa de l'article 19 de la Loi n° 1.165.

LES INVESTIGATIONS

Deux contrôles sur place ont été effectués en 2018 et ont concerné tous les deux un dispositif de vidéosurveillance.

La première investigation a fait suite à une plainte par laquelle la Commission a été informée que l'exploitant de l'établissement concerné avait indiqué à l'un de ses salariés qu'il avait installé des caméras afin de surveiller ses agissements.

Les constatations ont permis de s'assurer qu'aucun dispositif de vidéosurveillance n'était exploité, et que le responsable de l'établissement avait, à titre dissuasif, fait savoir qu'il avait mis des caméras.

Dans le second cas la CCIN a été alertée sur l'utilisation de caméras dans un commerce, sans obtention d'autorisation de mise en œuvre par la Commission, et dont les images seraient utilisées à des fins de contrôle des horaires de travail des salariés, ce que la CCIN interdit formellement.

Les investigations, réalisées en fin d'année 2018, ont révélé l'exploitation illégale d'un tel dispositif, de même que son utilisation à des fins de surveillance du travail, ainsi que du temps de travail des salariés.

De plus lors du contrôle le responsable des locaux a tenté de dissimuler des documents aux investigateurs.

Le Rapport mentionnant les irrégularités qui ont été relevées lors de ce contrôle a été notifié au responsable de traitement afin qu'il puisse faire part de ses observations sous un délai d'un mois, conformément à l'article 19 de la Loi n° 1.165.

Lesdites observations, reçues en toute fin d'année 2018, feront l'objet d'un examen attentif afin que le Président de la Commission puisse se prononcer sur les suites qui seront réservées à cette affaire.

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

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

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

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

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

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 2018 il a été procédé à 5 vérifications, dont 3 auprès de la Direction de la Sûreté Publique et 2 auprès du Service d'Information et de Contrôle sur les Circuits Financiers.

A l'issue de l'une d'entre elles les informations ont pu être portées à la connaissance du demandeur, après l'accord du Ministre d'Etat, dans la mesure où leur communication ne portait pas atteinte à la sécurité publique.

En fin d'année 2018 le Président de la Commission a été saisi d'une autre demande d'exercice du droit d'accès indirect auprès du SICCFIN pour laquelle les vérifications seront effectuées en 2019.

Il est par ailleurs à noter que, dans le cadre de la modification de la législation relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption intervenue au mois de juin 2018, le droit d'accès indirect peut désormais être exercé auprès des établissements assujettis à ces dispositions.

Toutefois en 2018 la CCIN n'a été saisie d'aucune demande de vérifications auprès de ces établissements.

LA NOTIFICATION À L'AUTORITÉ DE CONTRÔLE DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

Désormais obligatoire en application de l'article 33 du RGPD, la notification à l'Autorité de contrôle des violations de données à caractère personnel n'est pas une obligation résultant du droit interne monégasque.

Cependant cette obligation pèse sur les entités situées à Monaco soumises au RGPD compte tenu de son champ d'application extra territorial.

Au cours de l'année 2018 deux entités ont informé la CCIN de violations de données qu'elles traitaient.

La CCIN les a invitées à effectuer cette notification à la CNIL, Autorité européenne concernée dans la mesure où les données portaient majoritairement sur des personnes situées en France, et que la notification prévue par le RGPD doit obligatoirement s'effectuer auprès d'une Autorité de contrôle située en Union européenne.

Pour rappel à ce jour la seule obligation de notification à la CCIN concerne les violations de données personnelles traitées dans le cadre de l'échange automatique d'informations en matière fiscale.

LES DOSSIERS DU SECTEUR PUBLIC ET ASSIMILE

CCIN 6

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

Dans le prolongement de ses travaux consacrés aux échanges automatiques d'informations à des fins fiscales, la Commission a adopté une délibération n° 2018-002 du 17 janvier 2018 relative à la mise en place d'une plateforme dédiée (accessible à l'adresse https://eai.gouv.mc) destinée à recevoir les déclarations visées dans l'Ordonnance Souveraine n° 6.208 du 20 décembre 2016 portant application de la Convention concernant l'assistance administrative mutuelle en matière fiscale, de l'Accord multilatéral entre Autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers et du Protocole de modification de l'Accord entre la Communauté Européenne et la Principauté de Monaco prévoyant des mesures équivalentes à celles que porte la Directive 2003/48/CE. Celle-ci permet ainsi à la Direction des Services Fiscaux de contrôler le respect par les Institutions financières de Monaco de leurs obligations déclaratives et de diligences raisonnables.

Suite à ce premier traitement, la Commission a adopté une seconde délibération n° 2018-083 du 20 juin 2018 relative aux échanges automatiques d'informations entre Monaco et les juridictions soumises à déclarations via la plateforme CTS mise en place par l'Organisation de Coopération et de Développement Economiques (OCDE).

Dans une troisième délibération n° 2018-084 du 20 juin 2018 portant autorisation de transfert d'informations nominatives à destination de certaines juridictions ayant pour finalité « *Transmission d'informations à des fins fiscales entre Monaco et les juridictions soumises à déclaration* », la Commission a encadré les transferts de données vers des juridictions étrangères dites « *juridictions soumises à déclaration* » susceptibles d'être situées dans des pays ne disposant pas d'un niveau de protection adéquat.

Le Gouvernement Princier met régulièrement à jour sur un site internet une FAQ sur l'échange automatique d'informations à des fins fiscales : *https://www.gouv.mc/Action-Gouvernementale/Monaco-a-l-International/La-fiscalite-internationale/Foire-aux-questions-Faq-sur-l-echange-automatique-d-informations-en-matiere-fiscale.*

LA CCIN MODERNISE SON SITE INTERNET ET SON RÉPERTOIRE DES TRAITEMENTS

Pour répondre à l'évolution de ses missions ainsi qu'à l'accroissement du nombre de démarches des responsables de traitement la CCIN a souhaité moderniser son site Internet par l'ajout d'un certain nombre de fonctionnalités, telles que la mise en place d'un flux RSS et l'établissement de statistiques de navigation grâce à une gestion interne des cookies.

Elle a en a également profité pour faire évoluer son répertoire des traitements puisque celui-ci permet désormais aux responsables de traitement de gérer les habilitations des personnes en charge de remplir les formulaires et d'initialiser ou de modifier leur mot de passe. Ils peuvent également obtenir la liste des traitements en cours de dépôt et consulter la liste des traitements actifs ainsi que leur contenu, hormis les informations liées à la sécurité des traitements relatifs à l'article 11 de la Loi n° 1.165 du 23 décembre 1993. Enfin, les responsables de traitement peuvent faire évoluer un traitement existant.

Ces deux traitements ont reçu un avis favorable, respectivement par délibération n° 2018-086 en date du 20 juin 2018 pour la « *Gestion du site internet de la CCIN* » et délibération n° 2018-067 du 16 mai 2018 pour la « T*enue du Répertoire des Traitements* ».

LES TRAITEMENTS RELEVANT DE LA DIRECTION DU TRAVAIL

Par 3 délibérations en date du 17 janvier 2018, la Commission a levé les réserves qu'elle avait émises il y a plus de 10 ans pour trois traitements relevant de la Direction du Travail.

Elle s'est également prononcée sur la modification du traitement relatif à la gestion du « *dossier employeur* ».

Les déclarations d'accidents du travail

Le premier dossier comportant des réserves concernait l'enregistrement des déclarations d'accidents du travail qui avait fait l'objet d'un avis favorable en 2007 sous réserve de la modification des accès au traitement. Après avoir constaté que ces accès étaient désormais dévolus dans le respect de la Loi n° 1.165 du 23 décembre 1993, la Commission a toutefois demandé que la forme nominative des informations relatives aux salariés et aux employeurs soit supprimée 20 ans à compter du dépôt de déclaration de l'accident du travail, sauf lorsqu'il conduit à une peine criminelle. Dans ce cas, la durée de conservation pourra alors être portée à 35 ans.

Les permis de travail

Par délibération n° 2018.019, la Commission a pu constater que le cadre juridique concernant la circulation d'informations nominatives relatives aux demandeurs de permis de travail entre les Services de l'Administration intervenant dans le processus de délivrance était désormais établi. Elle a cependant demandé que l'information des personnes concernées soit rédigée dans le respect des mentions figurant à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, et que les durées de conservation soient modifiées.

La Commission a également demandé à la Direction de la Sûreté Publique de lui soumettre le traitement des enquêtes préalables, si celui-ci est effectué de manière automatisée. Par ailleurs, elle a recommandé qu'au sein des documents permettant de formaliser une demande d'embauchage, de renouvellement ou de modification d'un contrat de travail, communs à la Direction du Travail et à la Caisse de Compensation des Services Sociaux, seule la partie intéressant la Direction du Travail soit conservée dans le dossier papier des salariés.

Le dossier « *salarié régimes particuliers* »

Le dernier traitement ayant pour finalité « *Constitution du dossier « salarié régimes particuliers »* » n'est quant à lui désormais assorti que de simples

rappels concernant d'une part la collecte et la conservation de la copie de documents d'identité officiels et d'autre part certaines mesures de sécurité à respecter.

Le dossier employeur

Enfin, la Commission a approuvé par sa délibération n° 2018-017 la modification apportée au traitement ayant pour finalité « *Constitution du dossier employeur* » afin d'ajouter dans les données traitées concernant l'employeur, la possibilité de réaliser ses activités en télétravail dans le respect de la Loi n° 1.429 du 4 juillet 2016.

LE DISPOSITIF DE GESTION DES COURSES DES TAXIS EXPLOITÉ PAR LA DIRECTION DE L'EXPANSION ECONOMIQUE

Le rapport d'activité 2017 de la Commission (page 33) faisait état d'un contrôle relatif à l'exploitation du dispositif automatisé de gestion des courses de taxi, à l'issue duquel les irrégularités relevées avaient été notifiées au responsable de traitement, qui avait alors initié une mise en conformité.

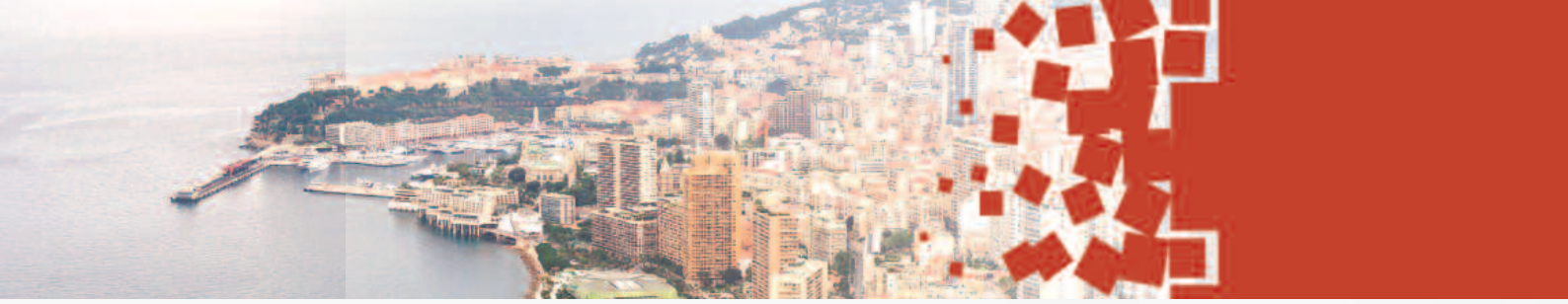
Celle-ci s'est traduite notamment par le dépôt le 15 décembre 2017, par le Ministre d'Etat, d'un traitement automatisé ayant pour finalité la « *Gestion du Service des courses de taxi* ».

Ce traitement est justifié par le respect d'une obligation légale, à savoir l'Ordonnance Souveraine n° 1.720 du 4 juillet 2008, l'Arrêté Ministériel n° 2014-329 du 16 juin 2014 fixant les modalités d'exercice du service minimum en application de l'article 23 de l'Ordonnance susvisée, ainsi que l'Arrêté Ministériel n° 2011-250 du 28 avril 2011 relatif aux conditions et modalités d'installation et d'utilisation de l'appareillage de communication des taxis.

Aux éléments présents dans les textes régissant la matière a été rajoutée une fonctionnalité de géolocalisation des taxis à des fins d'amélioration du service, par une meilleure allocation d'un véhicule proche à un client.

La Commission, dans sa délibération n° 2018-042 du 21 mars 2018 portant avis favorable à la mise en œuvre de ce traitement, a insisté sur la qualité de l'information dispensée aux chauffeurs vis-à-vis de ce dispositif, qui doit pouvoir être désactivé sur les temps de pause, mais aussi, d'une manière plus générale, sur celle mise à disposition des clients sur les différents canaux de réservation (deux sites internet, application mobile, téléphone), conformément à l'article 14 de la Loi n° 1.165.

Par ailleurs, elle a fixé la durée de conservation des informations de géolocalisation à deux mois, et celle des autres informations nominatives collectées à 1 an en lieu et place des 800 jours demandés.



Enfin, la Commission a également rappelé certaines exigences de sécurité, qu'elles soient techniques ou de confidentialité pour les tiers disposant d'un accès au traitement.

Elle a de plus précisé que seules les personnes dûment habilitées devaient avoir connaissance des informations nominatives exploitées dans ce dispositif.

LES CONTRÔLES ALIMENTAIRES, SANITAIRES ET VÉTÉRINAIRES MENÉS PAR LA DIRECTION DE L'ACTION SANITAIRE

Le 16 mai 2018, la Commission a émis un avis favorable à la mise en œuvre par la Direction de l'Action Sanitaire (DAS) d'un traitement automatisé ayant pour finalité « *Gestion des dossiers des contrôles alimentaires, sanitaires et vétérinaires* ». Justifié par une obligation légale à laquelle est soumis le responsable de traitement, à savoir l'article 2 de l'Ordonnance n° 5.640 du 14 décembre 2015 qui prévoit que la DAS est, entre autres, chargée d' « *assurer la prévention et le dépistage des maladies, ainsi que la veille sanitaire* », ce traitement permet aux fonctionnaires et agents de ce service de gérer l'ensemble des dossiers de plainte, de demande d'agrément, d'inspection, de contrôle ou encore d'autorisation qu'ils ont à connaître.

Concomitamment à cet avis, la Commission a également autorisé le transfert, vers les Autorités en charge dans le monde entier de la veille sanitaire ou vétérinaire, d'informations nominatives sur l'absence de dangerosité d'un produit ou animal lorsque des personnes ou entreprises souhaitent importer des marchandises ou voyager à l'étranger avec leur animal de compagnie.

LA GESTION DU CENTRE DE LOISIRS PRINCE ALBERT II ET DU PASS'SPORT CULTURE

La Direction de l'Education Nationale, de la Jeunesse et des Sports a remplacé l'application destinée à gérer le Centre de loisirs sans hébergement dont le traitement « *Gestion du Centre de Loisirs sans Hébergement* » a été légalement mis en œuvre en 2002 et modifié en 2008, par une nouvelle application dénommée « *Concerto* » ainsi que « *L'espace Loisirs* » accessible en ligne.

Le Centre de Loisirs Prince Albert II est une structure proposant des activités fonctionnant le mercredi après-midi et durant les vacances scolaires pour les enfants scolarisés à Monaco, dont les parents ont une activité professionnelle et le Pass'Sport Culture est destiné aux jeunes de 13 à 21 ans résidents ou scolarisés à Monaco proposant des activités sportives et culturelles durant les vacances d'été.

Le traitement comprend désormais plusieurs applications :

- une application interne, Concerto, qui gère elle-même les comptes utilisateurs et leurs habilitations, utilisée par le personnel habilité de l'Administration ;
- un espace Loisirs, portail utilisé par les parents pour inscrire leurs enfants au Centre de loisirs ou au Pass'Sport Culture ;
- un module dénommé, Diffusion permettant l'envoi ciblé en masse de notifications par email ;
- un module dénommé, CMO permettant le pointage de la présence horaire (arrivée/départ) des enfants sur tablettes.

Par délibération n° 2018-118 du 18 juillet 2018 le traitement ayant pour finalité « *Gestion du Centre de Loisirs Prince Albert II et du Pass'Sport Culture* » a reçu un avis favorable de la Commission.

LES TRAITEMENTS DE LA CAM

En 2018, la Compagnie des Autobus de Monaco (CAM) a soumis 2 traitements à l'avis de la Commission et une demande d'autorisation.

Conformément à l'article 7 de la Loi n°1.165 du 23 décembre 1993, la Commission a émis deux avis favorables concernant des traitements mis en œuvre par la CAM.

Gestion des allocations du fonds social et des achats de loisirs

Le premier avis rendu par délibération n° 2018-116 du 18 juillet 2018 ayant pour finalité « *Gestion des allocations du fonds social et des achats de loisirs* »

concerne les allocations du fonds social dont bénéficient les salariés de la société, conformément à l'Avenant n° 8 du 4 février 1969 à la Convention collective nationale du travail du 5 novembre 1945 instaurant un fonds social dans les entreprises occupant plus de 50 salariés.

Par le biais d'une plateforme permettant la gestion centralisée des bénéficiaires, sont proposés des prix promotionnels sur différents loisirs, tels que des spectacles, des activités sportives, des sorties éducatives et culturelles.

L'attention de la Commission s'est portée sur l'information préalable de personnes concernées, car la plateforme de la CAM renvoie automatiquement vers un site internet français *www.meyclub.com*. A cet égard le responsable de traitement indiquait que « *Les données d'identification et les informations personnelles sont automatiquement réinscrites* ».

La Commission a alors demandé que les personnes concernées soient informées que leurs informations sont communiquées audit site internet français.

Par ailleurs, constatant qu'un outil permettait de faire des statistiques et que le site utilisait des cookies, elle a demandé que les personnes concernées soient informées :

- de l'utilisation de Google Analytics par le site français et du fait que dès leur connexion, les données de navigation des bénéficiaires pouvaient se retrouver aux Etats unis, pays ne disposant pas d'un niveau de protection adéquat ;
- de manière plus précise relativement aux cookies (nature des cookies, manière permettant de s'en prévenir, conséquences, etc...).

Sur le plan de la sécurité, elle a demandé que :

- les identifiants et les mots de passe des administrateurs soient individuels et strictement personnels ;
- lors de l'activation de son compte ou la modification de son mot de passe, l'agent / bénéficiaire soit invité à saisir un mot de passe réputé fort ;
- les ressources du Comité du Fonds Social se trouvant sur le réseau informatique de la CAM soient protégées par des comptes utilisateurs individuels.

Gestion et établissement de la comptabilité

Le deuxième traitement ayant pour finalité « *gestion et établissement de la comptabilité* » a reçu un avis favorable par délibération n° 2018-115 du 18 juillet 2018.

Afin de satisfaire à ses obligations, la CAM a mis en place un logiciel destiné à contrôler et établir les recettes par agent-conducteur et à gérer les recettes et les dépenses des clients et des fournisseurs.

Outre le respect de ses obligations, le traitement a été justifié par la réalisation d'un intérêt légitime sans que ne soient méconnus les droits et libertés fondamentaux de la personne concernée. Utilisé dans un souci d'efficacité comptable, l'outil permet l'édition de rapports de gestion et « *des états financiers à date fixe ainsi que des états prévisionnels. Les exercices de rapprochements permettent de comparer les entrées et les sorties. Pour les recettes des chauffeurs, il permet la comparaison des ventes de titres effectuées à bord des bus avec le dépôt des recettes effectuées par les agents dans le coffre PROSEGUR* ». De ce fait, il contribue à la bonne gestion financière et administrative de la société.

La Commission, après avoir relevé que certaines informations complémentaires étaient collectées, a demandé que toutes les catégories de personnes

concernées (les salariés, les fournisseurs et les clients) soient informées, ce que la mention accessible en intranet ne permettait pas, seuls les salariés pouvant bénéficier d'une information.

Elle a ensuite relevé l'existence d'une interconnexion avec un traitement relatif à la gestion des accès et des habilitations non légalement mis en œuvre et a alors demandé que le traitement lui soit soumis dans les meilleurs délais.

S'agissant de la sécurité du traitement, elle a demandé qu'une journalisation des accès au traitement soit mise en place afin de pouvoir effectuer une vérification de ceux-ci. Elle a par ailleurs constaté que l'accès distant du prestataire était sécurisé.

Enfin, le traitement prévoyant l'envoi des informations aux Autorités fiscales françaises, la Commission a toutefois rappelé que cette communication ne pouvait se faire que par le biais de la Direction des Services Fiscaux de la Principauté conformément à l'article 20 de la Convention fiscale entre la France et la Principauté de Monaco du 18 mai 1963.

Géolocalisation des véhicules de transports publics

Par délibération n° 2018-117 du 18 juillet 2018 la Commission a autorisé conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, la mise en œuvre du traitement ayant pour finalité « *Géolocalisation des véhicules de transports publics urbains par le biais d'un système d'aide à l'exploitation et à l'information des voyageurs* », dénommé SAEIV (Système d'Aide à l'Exploitation et à l'Information des Voyageurs).

La demande concernait la mise en œuvre d'un dispositif permettant de géolocaliser les véhicules de transports publics urbains afin d'informer les passagers sur l'arrivée des véhicules en temps réel.

Les objectifs sont notamment de réguler les véhicules de transport en commun afin de respecter au mieux les horaires, de mettre à disposition des passagers aux arrêts de bus, à la gare, à l'hôpital, dans le bus, sur le site internet et sur l'application smartphone, des informations sur l'arrivée des véhicules ainsi que sur le temps d'attente.

Le dispositif contribue par ailleurs à effectuer le suivi du temps de travail effectif et la vérification du respect des trajets prévus, ainsi que le calcul de la vitesse des véhicules sur les tronçons spécifiques à des horaires particuliers permettant d'assurer respectivement le respect des engagements du service public et l'élaboration d'horaires réalistes et fiables.

Enfin il permet de déterminer la position d'un véhicule concerné en cas de réclamation et de vérifier les circonstances des accidents de la circulation impliquant un véhicule de la CAM.

Lors de l'examen du dossier, la Commission a relevé que l'application mobile destinée à obtenir des informations sur l'arrivée des véhicules, les horaires, la liste des arrêts et le temps d'attente, permettait également de géo-positionner l'usager lorsque celui-ci active son service de localisation et autorise l'application à y avoir accès, affichant l'emplacement des arrêts de bus et des distributeurs de tickets les plus proches.

En outre, cette application possédant l'outil de statistiques Google Analitycs, la Commission a indiqué que les informations des utilisateurs étaient de ce fait transférées aux Etats Unis d'Amérique, pays ne disposant pas d'un niveau de protection adéquat au sens de la législation monégasque.

La Commission a alors rappelé que ces transferts ne pourront être effectués qu'après l'obtention d'une autorisation de transfert.

Elle a également relevé que l'adresse IP des utilisateurs de l'application était collectée et a par ailleurs demandé que l'information préalable soit dispensée à l'ensemble des personnes concernées conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

LA VIDÉOPROTECTION URBAINE EXPLOITÉE PAR LA DIRECTION DE LA SÛRETÉ PUBLIQUE

Par sa délibération en date du 3 septembre 2018, la Commission a émis un avis favorable à la mise en œuvre par le Ministre d'Etat du traitement

automatisé d'informations nominatives ayant pour finalité « *Mise en œuvre et exploitation du système de vidéoprotection urbaine par la Direction de la Sureté Publique* ».

En vertu de l'article 7 alinéa 2 de la loi n°1.165 du 23 décembre 1993, « *les traitements visés à l'article 11 ne donnent lieu à publication que le sens de l'avis de la commission et de la décision de l'autorité ou de l'organe compétent* ». Le présent traitement intéressant la sécurité publique, la disposition légale susmentionnée s'applique. En conséquence, l'avis motivé relatif à cette demande d'avis n'a pas fait l'objet d'une publication au Journal de Monaco.

LA VIDÉOSURVEILLANCE DE LA SALLE DE SPORT HERCULE FITNESS CLUB

Par sa délibération n°2018-154 en date du 17 octobre 2018, la Commission a émis un avis favorable à la mise en place par la Commune de Monaco d'un système de vidéosurveillance de la Salle de Sport Hercule Fitness Club. Elle a toutefois

demandé à ce que la caméra située à l'extérieur ne filme que les abords immédiats du portail et du portillon d'accès.

La Commission a par ailleurs demandé à ce qu'une journalisation automatisée des accès aux enregistrements soit mise en place et que l'affichage soit impérativement complété afin d'indiquer les modalités d'exercice du droit d'accès en Principauté.

Enfin, elle a interdit l'enregistrement des images des caméras filmant l'intérieur des salles dédiées à la pratique du sport, puisque de telles salles sont avant tout des lieux de bien-être et de loisir mis à la disposition des clients.

LE PACTE NATIONAL POUR LA TRANSITION ENERGÉTIQUE

Le 21 novembre 2018, la Commission a émis un avis favorable à la mise en œuvre par la Mission pour la Transition Energétique du traitement automatisé d'informations nominatives ayant pour finalité « *Permettre aux usagers d'adhérer en ligne au Pacte National pour la Transition Energétique* ». Cette cellule administrative du Département de l'Equipement, de l'Environnement et de l'Urbanisme est en charge de la planification et de la mise à jour de la stratégie de transition énergétique et a notamment pour objectif la réduction des émissions de gaz à effet de serre, aux fins de respecter les dispositions du Protocole de Kyoto.

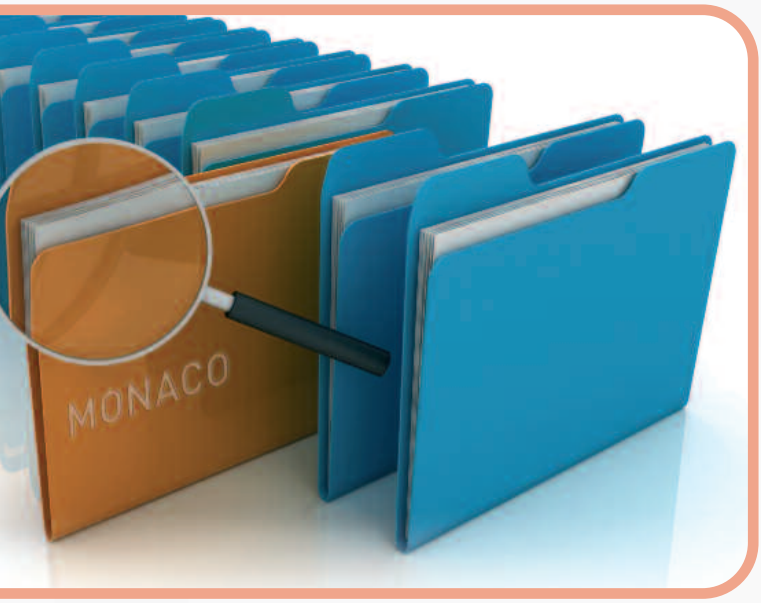
La Commission a pu constater que ledit traitement était justifié par le consentement des nouveaux adhérents, formalisé par l'obligation préalable d'accepter les conditions générales d'utilisation en ligne. Elle a également pris acte de la possibilité pour les personnes concernées par cette démarche d'adhésion de consentir à afficher leurs noms et prénoms sur le site officiel de la Mission pour la Transition Energétique, à condition qu'aucune réponse (choix oui/non) ne soit cochée au préalable.

Ce traitement a pour spécificité de collecter non seulement des informations relatives à l'identité et aux coordonnées de la personne, mais également des données concernant ses habitudes de vie et de consommation, afin d'estimer ses émissions personnelles de gaz à effet de serre.

S'agissant du traitement « *Gestion du compte permettant aux usagers d'entreprendre des démarches par téléservices* » permettant aux usagers d'accéder de manière sécurisée à cette démarche de transition énergétique, la Commission a demandé que les futurs adhérents soient invités à renseigner, lors de la création de leurs comptes, des mots de passe réputés forts, afin de tenir compte des exigences techniques et organisationnelles actuelles.

LA GESTION DU REGISTRE DES BÉNÉFICIAIRES EFFECTIFS PAR LA DIRECTION DE L'EXPANSION ECONOMIQUE

Dans le prolongement de ses travaux relatifs à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, la Commission a adopté une délibération n° 2018-175 du 21 novembre 2018 relative à un traitement automatisé d'informations nominatives ayant pour finalité la « *Gestion d'un registre des bénéficiaires effectifs des sociétés commerciales, groupements d'intérêt économique et sociétés civiles de droit monégasque* » exploité par la Direction de l'Expansion Economique.



En effet, conformément à l'article 21 alinéas 3 et 4 de 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 « *les sociétés commerciales et les groupements d'intérêt économique immatriculés au répertoire du commerce et de l'industrie ainsi que les sociétés civiles inscrites sur le registre spécial tenu par le service du répertoire du commerce et de l'industrie, sont tenus d'obtenir et de conserver les informations adéquates, exactes et actuelles sur leurs bénéficiaires effectifs définis au premier alinéa et sur les intérêts effectifs détenus. Les personnes morales et entités visées au précédent alinéa sont tenues de fournir, aux organismes et personnes visés aux articles premier et 2, pour l'accomplissement des obligations de la présente loi, toutes les informations adéquates, exactes et actuelles qu'elles possèdent sur leurs bénéficiaires effectifs* ».

Par ailleurs, l'article 22 alinéa 1er de la Loi n° 1.362 du 3 août 2009 dispose que « *les personnes morales et entités visées au troisième alinéa de l'article précédent communiquent les informations sur les bénéficiaires effectifs au Ministre d'État, aux fins d'inscription sur un répertoire spécifique intitulé « registre des bénéficiaires effectifs », annexé au répertoire du commerce et de l'industrie et les mettent à jour régulièrement* ».

L'objectif du registre des bénéficiaires effectifs, qui trouve son origine dans la Directive n° 2015/849/UE du 20 mai 2015 du Parlement et du Conseil européen dite « *4ème directive anti-blanchiment* », est de favoriser la transparence économique, ainsi que de lutter contre le blanchiment de capitaux et le financement du terrorisme. Pour ce faire, il vise à identifier les personnes physiques qui contrôlent en dernier ressort une société ou une entité juridique et bénéficient effectivement de son activité.

Dans le cadre de sa délibération n° 2018-175 du 21 novembre 2018 portant avis favorable à la mise en œuvre de ce traitement la Commission a souligné que les accès aux informations traitées devaient être conformes aux textes et que l'information préalable devait être effectuée auprès de l'ensemble des personnes concernées.

LA GESTION DES ALLOCATIONS POUR CHARGES DE FAMILLE PAR LE SERVICE DES PRESTATIONS MÉDICALES DE L'ETAT

Par sa délibération n° 2018-210 du 19 décembre 2018, la Commission a émis un avis favorable à la mise en œuvre par le Service des Prestations Médicales de l'Etat (SPME), organisme chargé de gérer les prestations accordées par l'Etat au titre des prestations familiales et autres avantages sociaux y afférents, du traitement automatisé d'informations nominatives ayant pour finalité « *Attribution, calcul et suivi des allocations pour*

charges de famille ». Ce dernier concerne les allocataires (qui bénéficient du droit aux allocations), les attributaires (à qui sont versées les allocations), ainsi que les enfants de foyer ; soit environ 10 000 personnes.

En vertu de l'Arrêté Ministériel n° 2018-952 du 10 octobre 2018 portant application de l'Ordonnance Souveraine n° 7.155 du 10 octobre 2018 relative à l'octroi des allocations pour charges de famille aux fonctionnaires et agents de l'État et de la Commune, d'autres pièces, non mentionnées au sein du présent traitement, peuvent être communiquées : extrait intégral de naissance, feuillet d'examen prénatal, etc. Cependant, ces documents sont en l'espèce traités et conservés sous format papier et ne sont pas numérisés. Leur traitement n'est donc pas automatisé et ne doit pas être soumis à formalité auprès de la Commission.

Le responsable de traitement ayant indiqué que les informations seraient conservées cinq années après le dernier versement des allocations, la Commission, estimant que les informations relatives aux bulletins de paiement et au foyer de l'allocataire (caractéristiques financières, adresse, attributaires associés, enfants, etc.) doivent être supprimées tous les cinq ans glissants, a demandé que les durées de conservation établies par le SPME soient modifiées, afin de respecter celles préconisées par la Commission.

LA DIRECTION DE LA PROSPECTIVE DE L'URBANISME ET DE LA MOBILITÉ ET LE SUIVI DES LETTRES DE COMMANDE, MARCHÉS D'ÉTUDE ET CONVENTIONS

Le 19 décembre 2018, la Commission a émis, par le biais de sa délibération n° 2018-209 un avis favorable à la mise en œuvre par la Direction de la Prospective, de l'Urbanisme et de la Mobilité (DPUM) du traitement automatisé d'informations nominatives ayant pour finalité « *Suivi et contrôle des lettres de commande, des marchés d'étude et des conventions* ».

Ce traitement permet à l'organisme de maitriser et de rationaliser le suivi des commandes, marchés et conventions de multiples projets et études. En effet, l'article 2 de l'Ordonnance n°1.463 du 7 janvier 2008 portant création de la DPUM octroie à cette dernière de nombreuses missions : « *mener les études de programmation des projets d'urbanisme publics* », « *élaborer des stratégies et plans de mobilité* », « *mener toutes études prospectives s'inscrivant dans son champ de compétence dans le but d'améliorer le cadre de vie et la mobilité, ...* », nécessitant l'établissement d'une procédure de contrôle et de supervision automatisée pour lesdites opérations.

Dans le cadre de sa délibération, la Commission a par ailleurs rappelé qu'en dépit des éléments indiqués par le responsable de traitement dans une pièce jointe au dossier, les personnes concernées ne disposent pas d'un droit d'opposition à l'exploitation de leurs informations.

LE CHPG ACCÉLÈRE LA MISE EN CONFORMITÉ DE SES TRAITEMENTS

Le Centre Hospitalier Princesse Grace a repris sa démarche de mise en conformité de ses traitements automatisés d'informations nominatives avec 21 dossiers déposés au cours de l'année 2018 concernant des éléments essentiels au fonctionnement de l'établissement.

La première demande concernait ainsi un traitement ayant pour finalité « *Gestion des attributions des places de parking* » mis en oeuvre afin de simplifier le quotidien des salariés de l'hôpital en leur permettant de pouvoir bénéficier de places de stationnement réservées par le Gouvernement Princier dans différents parkings situés à proximité de l'établissement et de ses structures détachées. Par délibération n° 2018-046 en date du 18 avril 2018, la Commission a émis un avis favorable, en demandant toutefois que les informations des personnes n'ayant pas donné suite à l'attribution d'un abonnement soient supprimées une année après la notification de ladite attribution.

Le même jour, la Commission a émis un avis favorable au traitement ayant pour finalité « *Gestion des admissions à la crèche* » en demandant là aussi que la forme des informations permettant l'identification des personnes concernées soit supprimée un an après l'intégration de l'enfant au sein de la crèche ou bien après la notification aux parents de la suite non favorable réservée à la demande.

Le 20 juin 2018, la Commission a émis 3 nouveaux avis favorables concernant des traitements ayant respectivement pour finalité « *Gestion du temps de travail des personnels non médicaux* », « *Gestion des formations du personnel non médical* » et « *Gestion des attributions de logement* ». Pour ce dernier, la Commission a toutefois demandé que les informations des personnes n'ayant pas donné suite à l'attribution d'un logement soient supprimées une année après la notification de ladite attribution.

Un mois plus tard, sept nouveaux traitements ont fait l'objet d'un avis favorable de la Commission. Si les traitements ayant respectivement pour *finalité « Gestion des missions d'assistante sociale »*, « *Circuit informatisé du médicament* » et « *Contrôle d'accès par badge non biométrique aux locaux Monégasques du CHPG* », n'ont fait l'objet d'aucune remarque particulière, la Commission a toutefois émis plusieurs réserves concernant le traitement ayant pour finalité « *Vidéosurveillance de tous les sites monégasques du CHPG* ».

Elle a ainsi demandé qu'un affichage (pictogramme) soit apposé dans les salles d'attente, dans le box des urgences et dans les autres pièces où se trouvent des caméras filmant uniquement au fil de l'eau, sans aucun enregistrement des images, afin que les patients s'y trouvant soient informés de la présence desdites caméras.

Elle a également demandé que les identifiants et les mots de passe des administrateurs permettant l'accès au système de vidéosurveillance soient nominatifs.

Enfin, la Commission a demandé que le traitement lié au système anti-fugue (boucle-sèche) lui soit soumis dans les plus brefs délais si celui-ci comporte des informations directement ou indirectement nominatives.

Par ailleurs, dans sa délibération n° 2018-108, concernant la gestion du questionnaire d'appréciation des séjours hospitaliers, la Commission a, en l'absence de justification, fixé la durée de conservation des données provenant de ce questionnaire, à 2 ans, sous forme nominative, à compter de leur collecte. Ce questionnaire n'a en effet d'autres fonctionnalités que d'identifier les éventuels points perfectibles dans le cadre de l'amélioration de la qualité et de la sécurité des soins, d'établir des statistiques (non nominatives) semestrielles et de diffuser annuellement les résultats du questionnaire.

Concernant le traitement ayant pour finalité « *Gestion des services de téléphonie et enregistrement de certaines conversations téléphoniques* », la Commission a tenu à rappeler que chaque administrateur devait avoir son propre identifiant et mot de passe nominatifs et qu'un message d'accueil devait être mis en place afin d'informer tout appelant extérieur de l'enregistrement de la conversation.

Elle a par ailleurs rappelé que le PABX devait régulièrement être mis à jour après chaque synchronisation du nom de l'utilisateur (interne et externe « *patients* ») avec le système AS400 (liste nominative attribuée aux postes téléphoniques dans le système informatique), et que les tickets (ID Appelant, ID Appelé) doivent avoir leurs 4 derniers numéros occultés lors de l'extraction de l'archivage.

Enfin, la Commission a recommandé qu'une procédure relative au droit d'accès par voie électronique soit mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel soit effectivement la personne concernée par les informations.

Quatre nouveaux avis favorables ont été rendus par la Commission lors de sa réunion du 19 septembre 2018 concernant les traitements ayant respectivement pour finalité « *Gestion des patients en hospitalisation soins ou traitements à domicile* », « *Gestion des rendez-vous patients* », « *Organisation et suivi du comité de gestion des œuvres sociales* » et « *Gestion de la crèche* ».

Pour ce dernier, les Commissaires ont toutefois fixé la durée de conservation des données de santé et celles liées au régime alimentaire à un an après le départ des enfants.

Le 17 octobre 2018, la Commission a émis trois avis favorables. Pour le traitement ayant pour finalité « *Gestion de la facturation des repas au self* », elle a cependant demandé à ce que tout utilisateur de l'application « *Self* » s'authentifie à chaque connexion à l'application et se déconnecte en fin d'utilisation permettant ainsi à l'utilisateur suivant de s'identifier et s'authentifier afin de se connecter au système. La Commission a par ailleurs demandé que les logs de connexion des personnes affectées à la caisse ne soient conservés que 1 an.

Concernant la « *Gestion du dossier obstétrique informatisé du CHPG* », elle a demandé que le traitement ayant pour finalité « *Gestion des centrales de surveillance du CHPG* » lui soit soumis dans les plus brefs délais.`

En outre, s'agissant du traitement ayant pour finalité « *Prise de commande des repas patients et accompagnants* », la Commission a demandé qu'une procédure de sécurisation des tablettes utilisées par le service hôtelier soit mise en place en cas de vol ou de perte desdites tablettes.

Un autre avis favorable a été rendu par la Commission le 21 novembre 2018, concernant cette fois le traitement ayant pour finalité « *Plate-forme de communication multicanal modulaire* » qui permet de gérer de manière centralisée les messages SMS en émission ainsi que les fax en émission et réception et d'assurer leur traçabilité. Enfin, la Commission a terminé l'année en émettant deux avis favorables à la mise en œuvre de deux traitements ayant respectivement pour finalité « *Gestion des patients en anesthésie* » et « *Gestion des centrales de surveillance* ». Pour ce dernier, elle a cependant demandé que le traitement lié à la gestion des tickets lui soit soumis dans les plus brefs délais.

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

Cette année, la Commission a été saisie de 10 recherches dans le domaine de la santé ; 9 déposées par le Centre Hospitalier Princesse Grace (CHPG) et 1 soumise par Centre d'Hémodialyse Privé de Monaco (CEHPM).

Recherches biomédicales

5 nouvelles recherches biomédicales mises en œuvre par des promoteurs représentés en Principauté par le CHPG ont ainsi fait l'objet d'un avis favorable de la CCIN.

La première, dénommée « *Etude ARTESIA* », a pour but de déterminer le traitement le plus efficace pour prévenir un accident vasculaire cérébral (AVC) ou une embolie systémique chez les patients ayant souffert d'au moins un épisode d'un trouble du rythme cardiaque appelé fibrillation auriculaire (FA) infraclinique détecté par un stimulateur cardiaque, un défibrillateur intracardiaque ou un moniteur cardiaque implantable. Cette étude a fait l'objet d'un avis favorable de la Commission le 21 mars 2018 qui a cependant demandé que la communication des données chiffrées et du mot de passe soit effectuée par deux canaux distincts.

Par délibération n° 2018-039 du 21 mars 2018, la Commission a également émis un avis favorable à la mise en œuvre d'une recherche dénommée

« *Etude REACH* » qui a pour objectif principal de démontrer que le traitement par avelumab en combinaison avec le cetuximab et la radiothérapie (RT) est supérieur aux traitements standards cisplatine-RT et/ou cetuximab-RT seuls, en termes de survie sans progression chez les patients ayant un carcinome épidermoïde localement avancé de la tête et du cou.

Cet avis a toutefois été assorti d'un certain nombre de demandes de la part de la Commission, à savoir que :

- le mois de naissance des patients soit supprimé du traitement, sauf pour les personnes ayant 18 ans l'année de l'inclusion afin de permettre à l'investigateur de démontrer le respect des critères d'inclusion ;
- le formulaire de consentement soit modifié afin d'indiquer que le patient peut signaler au médecin qu'il souhaite, lors de son retrait de l'étude, la suppression de ces données et que ce souhait sera pris en compte ;
- le mot de passe pour lire le fichier zip codé soit communiqué par un moyen autre qu'un message électronique ;
- le patient puisse s'opposer à la conservation de son échantillon tumoral à la fin de la recherche.

Le 18 juillet 2018, l' « *Etude ROC-SpA* » qui pour objectif principal d'identifier la meilleure stratégie de traitement de la spondylarthrite axiale après un premier échec du traitement par un anti-TNF (bio médicament), a reçu un avis favorable. Dans sa délibération, la Commission a cependant relevé que dans le cadre de cette étude, une sérothèque (banque de sang) allait être constituée afin d'enrichir la collection d'échantillons déjà existants du Service de Rhumathologie du CHU de Saint-Etienne. Ces échantillons seront

utilisés ultérieurement pour « *doser des nouveaux marqueurs impliqués dans les mécanismes des maladies inflammatoires* ».

Si la constitution de cette sérothèque fait bien l'objet d'un consentement spécifique, la Commission a cependant constaté que ledit document ne mentionne pas, contrairement à la note d'information, la possibilité pour le patient de demander à tout moment la destruction de ses échantillons. Elle a donc demandé que ce formulaire de consentement soit modifié en conséquence.

Lors de sa réunion en date du 21 novembre, la Commission a émis un autre avis favorable, concernant cette fois l'étude « *Procode* » dont l'objectif principal est d'estimer le pourcentage et la valeur prédictive positive du dosage de la progastrine pour le dépistage de cancers à des stades précoces

chez des volontaires sains asymptomatiques, venant faire un dépistage du côlon au CHPG, en demandant toutefois que le « *Consentement éclairé* » soit modifié afin de préciser que « *le droit d'accès, de rectification, d'opposition, de limitation et d'effacement des données* » peut s'exercer directement « *auprès du médecin signataire du consentement du patient* ».

Enfin, la Commission a émis un avis favorable à l'étude « *SURPASS* » et autorisé les 4 demandes de transfert de données vers les Etats-Unis et l'Inde, pays ne disposant pas d'un niveau de protection adéquat, qui lui ont été soumises concomitamment.

Cette étude a pour objectif de démontrer l'impact du sécukinumab sur la progression de l'atteinte structurelle au niveau de la colonne vertébrale, mesurée par le score mSASSS, chez des patients atteints d'une spondylarthrite axiale (SA).

La Commission a toutefois formulé plusieurs réserves concernant l'information préalable des personnes concernées. Elle a ainsi demandé que les deux formulaires de consentement soient modifiés afin d'indiquer qu'en cas de retrait les données déjà collectées seront conservées et traitées et que le patient peut à tout moment demander la destruction de ses échantillons biologiques. Par ailleurs, la Commission a demandé que le document d'information et les deux formulaires de consentement soient complétés afin d'indiquer que des transmissions d'informations se feront vers des destinataires situés en France, en Angleterre, en Bulgarie, aux Etats-Unis et en Inde pour permettre aux patients d'être informés de ces transferts et d'y consentir de manière libre et éclairée.

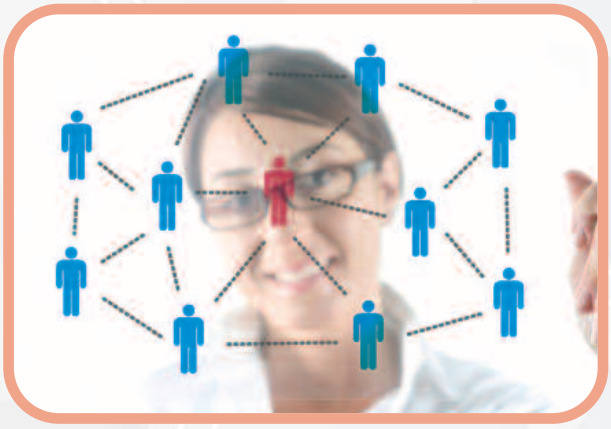
Recherches non biomédicales

Parallèlement, la Commission a émis 4 avis favorables concernant la mise en œuvre de recherches non biomédicales soumises par le CHPG.

Le premier avis a été rendu le 19 septembre 2018. Il concernait la « *COHORTE VNI* » dont objectif principal est d'analyser les données cliniques justifiant la prescription d'une ventilation non invasive (VNI) chez des patients insuffisants respiratoires. Après avoir constaté que les données relatives à l'identité du patient n'étaient pas seulement renseignées sur un document papier mais été également saisies par le médecin investigateur du CHPG dans un espace personnel et sécurisé de l'eCRF afin de faciliter une correspondance entre l'identité du patient et les données pseudonymisées, la Commission a demandé que seul le numéro d'inclusion du patient soit traité de manière automatisée.

Le même jour, un avis favorable a été émis concernant l'étude observationnelle « *RHAPSODY* » destinée à collecter des informations sur

la structure et le rythme du coeur des patients pour étudier un nouveau logiciel pour le système de cartographie Rhythmia. Pour cette étude, la société en charge de vérifier si l'algorithme détecte les mêmes troubles du rythme cardiaque que ceux détectés par le médecin du CHPG, étant localisée dans un pays ne disposant pas d'un niveau de protection adéquat, la Commission a donc émis concomitamment une autorisation de transfert des données collectées dans le cadre de ladite étude vers les Etats-Unis.



La Commission a également émis un avis favorable le 17 octobre 2018 à la mise en œuvre de la recherche observationnelle « *VERONE* » qui a pour objectif principal de décrire l'efficacité du vénétoclax chez des patients souffrant de leucémie lymphoïde chronique. Elle a cependant demandé que le formulaire de consentement soit modifié afin d'indiquer que le patient a le droit de s'opposer à l'utilisation des données non encore publiées ou communiquées, et que la communication des identifiants et des mots de passe soit effectuée par deux canaux distincts.

Par délibération n° 2018-194 en date du 19 décembre 2018, la Commission a émis un avis favorable à la mise en œuvre de l'étude « *FACIL-VAA* ».

Présentée par la Société Française de Recherche et Médecine du Sommeil (SFRMS), cette étude a pour objectif principal d'évaluer l'impact du traitement par Ventilation Auto-Asservie (VAA) sur la qualité de sommeil de patients avec un syndrome d'apnée du sommeil central ou combiné hors insuffisance cardiaque systolique à fraction d'éjection altérée. Elle devrait concerner une dizaine de patients traités au sein du service de pneumologie du CHPG.

La Commission a demandé que le formulaire de consentement soit complété afin d'indiquer qu'en cas de retrait de consentement, les données recueillies préalablement à ce retrait pourront ne pas être effacées et pourront continuer à être traitées dans le cadre de l'étude. Elle a également recommandé que la communication des données pseudonymisées chiffrées et des clés déchiffrement soit effectuée par deux canaux distincts.

Enfin, lors de la même séance, la Commission a émis un avis favorable à la mise en œuvre par le CEHPM d'une étude dont l'objectif principal est de déterminer l'impact du « *porte-saveur* » sur la variation de phosphorémie et dont les objectifs secondaires sont d'évaluer l'impact du « *porte-saveur* » sur la consommation de chélateurs de phosphore, le profil biologique des patients (IPAQSS) et la qualité de vie des patients.

Dénommée « *Etude PUCE* », cette recherche en soins courants concernera les patients hémodialysés chroniques et dialysés 3 fois par semaine au Centre d'Hémodialyse Privé de Monaco (CHPM) ou au CHPG, ainsi que les médecins investigateurs de néphrologie du CHPM et du CHPG et les personnels intervenant au cours de l'étude sur autorisation du médecin investigateur.

La Commission a formulé des observations relatives aux délais de conservation des mots de passe, devant varier en fonction de leur robustesse.

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

CCIN 7

LA MODIFICATION DES TEXTES RELATIFS À LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX, LE FINANCEMENT DU TERRORISME ET LA CORRUPTION

Dans 2 délibérations n° 2018-032 du 21 février 2018 relative au projet de Loi renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et n° 2018-098 du 18 juillet 2018 relative au projet d'Ordonnance Souveraine portant modification de l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, la Commission a eu l'occasion d'analyser les évolutions de cette règlementation inspirée de la Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, dénommée « *4ème Directive* ».

A cet égard, la Commission a constaté que ces modifications avaient pour objet d'aligner la règlementation monégasque sur les derniers standards internationaux régissant la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption (LAB-FT-C) et qu'elles avaient également des inférences sur différents textes tels que la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, la Loi n° 214 du 27 février 1936 sur les trusts, le Code pénal et le Code de procédure pénale, la Loi n° 1.355 du 23 décembre 2008 concernant les associations et les fédérations d'associations, la Loi n° 56 du 29 janvier 1922 sur les fondations et la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives.

Elle n'a pas manqué de relever notamment l'élargissement du champ des entités assujetties, ainsi que des éléments devant faire l'objet d'un signalement au SICCFIN.

Compte tenu des conséquences pour les personnes concernées de la mise en œuvre à leur égard des dispositions en matière de LAB-FT-C, la Commission a souligné qu'il importait que les textes régissant ce domaine soient suffisamment précis pour donner lieu à une application uniforme et prévisible.

LES MODIFICATIONS DE LA LÉGISLATION RELATIVE À L'AIDE À LA FAMILLE MONÉGASQUE ET À L'AIDE SOCIALE

Dans le cadre de la refonte des mesures relatives à l'aide à la famille monégasque et à l'aide sociale, le Ministre d'Etat a saisi la Commission des dispositions ayant vocation à renforcer la procédure de contrôle de la réalité des déclarations effectuées par les demandeurs d'aides sociales afin de permettre au Service instructeur de la demande de s'adresser aux autres Services administratifs pour obtenir les informations utiles à la vérification de la situation du requérant.

Dans sa délibération n° 2018-172 du 17 octobre 2018 portant avis sur les mesures envisagées, la Commission a relevé que les situations des personnes sollicitant le versement des prestations concernées pouvaient nécessiter la communication de justificatifs relatifs à des informations extrêmement personnelles portant sur les demandeurs ou sur leurs proches (solitude, indigence, situation familiale, ...).

Aussi, sans remettre en cause la légitimité des vérifications du bien-fondé de l'octroi des aides sociales, elle a indiqué qu'il importait que les communications d'informations par les Services de l'Etat soient encadrées par des dispositions suffisamment lisibles, précises et prévisibles pour les personnes concernées.

Compte tenu de la sensibilité des informations pouvant être demandées par le Service instructeur de la demande d'aide sociale, elle a également souligné qu'il importait de préciser explicitement la qualité des Agents relevant du Service instructeur de la demande, habilités à demander la communication d'informations auprès d'autres Services.

La Commission a pu constater que ces préconisations ont été prises en compte lors de la publication de la Loi n° 1.465 du 11 décembre 2018 relative à l'aide à la famille monégasque et à l'aide sociale.

A cet égard elle se réjouit que le Rapport de la Commission des Droits de la Femme et de la Famille du Conseil National ait repris à son compte les observations formulées par la CCIN.

Par ailleurs la Commission avait également souligné qu'une attention toute particulière devait être apportée aux mentions d'informations à insérer dans l'ensemble des formulaires de demandes d'aides sociales.

L'AVIS DE LA COMMISSION SUR LE PROJET DE LOI RELATIVE À LA FIN DE VIE

Saisie par le Ministre d'Etat le 2 août 2018 d'un projet de Loi relative à la fin de vie, la Commission a émis un avis par délibération n° 2018-201 en date du 19 décembre 2018.

Ce projet a pour vocation de compléter le cadre juridique en vigueur en Principauté concernant ce sujet très sensible en détaillant tout d'abord les règles applicables en matière de refus d'acharnement thérapeutique, mais également en matière de soins palliatifs, et d'adapter à ces situations particulières les règles générales applicables au consentement et à l'information en matière médicale prévues par la Loi n° 1.454 du 30 octobre 2017.

Si elle a constaté que les dispositions envisagées par le projet de Loi étaient pour la plupart similaires à celles contenues dans les Lois françaises Leonetti et Leonetti-Claeys des 22 avril 2005 et 2 février 2016, en prévoyant notamment la possibilité pour le patient de rédiger des directives anticipées, la Commission a cependant relevé que celles-ci ont un champ d'application plus restreint puisqu'elles ne sont ouvertes qu'aux personnes atteintes « *d'une affection grave, irréversible et incurable* ».

En effet, en France, cette faculté est offerte aux personnes « *a priori* » ; c'est-à-dire avant que celles-ci soient atteintes d'une maladie incurable.

Dans ce cas précis, la Commission, suivant le raisonnement énoncé par le projet de Loi, a constaté que le souhait du patient exprimé par le biais de ces directives, « *à une époque où une affection grave, irrésistible et incurable ne lui a pas encore été diagnostiquée* », est relatif dès lors à un évènement futur, ce qui ne peut s'assimiler, selon le texte, à une volonté éclairée.

La Commission a par ailleurs noté que cette exclusion des patients dont le pronostic vital n'est pas engagé lors de l'élaboration de la déclaration de fin de vie est conforme au droit européen des droits de l'homme. En effet, compte tenu de la complexité d'un tel sujet et de l'absence de consensus en la matière entre les Etats membres du Conseil de l'Europe, la Cour européenne des droits de l'homme leur a accordé une marge d'appréciation, en laissant le soin aux Autorités internes « *d'établir les souhaits du patient conformément à la loi nationale* » (affaire Lambert et autres contre France, 5 juin 2015).

En outre, la Commission a constaté que la possibilité de rédiger des directives anticipées n'avait pas vocation à être octroyée aux mineurs, à la différence des majeurs sous tutelle par l'intermédiaire de leur représentant. Toutefois le projet de Loi prévoit expressément la faculté pour le mineur de consentir à un acte ou traitement qui résulterait d'une obstination déraisonnable.

En matière de consentement la Commission a souligné que la capacité octroyée à chacun des patients de réviser ou de révoquer cette déclaration et la mise en œuvre d'un droit à l'information renforcée remplissaient les conditions prévues en droit positif monégasque permettant de constituer un consentement « *libre et éclairé* ».

Enfin la Commission, constatant la possibilité pour la personne concernée de déposer sa déclaration sur un registre central destiné à recueillir des déclarations émanant de patients atteints d'une affection grave, irréversible et incurable, a tenu à rappeler la nécessité pour le responsable de traitement de sécuriser de manière stricte l'exploitation de ce registre afin d'en garantir l'intégrité et la confidentialité.

LE PROJET D'ORDONNANCE SOUVERAINE EN MATIÈRE D'ACTION DISCIPLINAIRE DEVANT LE CONSEIL DE L'ORDRE DES MÉDECINS

Dans une délibération n° 2018-191 du 19 décembre 2018, la Commission a rendu un avis sur un projet d'Ordonnance Souveraine relative à l'instruction d'une action disciplinaire devant le Conseil de l'Ordre des Médecins. A cette occasion, la Commission est revenue sur un certain nombre de notions essentielles telles que le secret médical, les données de santé et le consentement du patient. Aussi, elle a pu rappeler les conditions de la levée du secret professionnel qui est régi à Monaco par les dispositions de l'article 308 du Code pénal.

De même les contours des missions dévolues au médecin inspecteur de santé publique ont également été évoqués.

L'Ordonnance Souveraine telle que publiée suite à la consultation de la Commission prévoit que l'accès ou la communication de données de santé ne peut s'effectuer qu'après le recueil du consentement écrit des patients concernés.

LA CRÉATION D'UN NOUVEAU TÉLÉSERVICE MIS EN ŒUVRE PAR LA DIRECTION DES SERVICES FISCAUX

Par délibération n° 2018-001 du 17 janvier 2018 portant avis sur la consultation du Ministre d'Etat relative au projet d'Arrêté Ministériel portant application de l'Ordonnance Souveraine n° 6.208 du 20 décembre 2016 portant application de la Convention administrative mutuelle concernant l'assistance administrative mutuelle en matière fiscale, de l'Accord multilatéral entre Autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers et du Protocole de modification de l'Accord entre la Communauté européenne et la Principauté de Monaco prévoyant des mesures équivalentes à celles que porte la Directive 2003/48/CE, modifiée, la Commission a émis un avis sur la création d'un téléservice mis en œuvre par la Direction des Services Fiscaux et permettant aux Institutions financières déclarantes d'effectuer les déclarations mentionnées à l'article 3 de l'Ordonnance Souveraine n° 6.208 du 20 décembre 2016, modifiée.

Ce téléservice mis en œuvre par la Direction des Services Fiscaux est régi par les dispositions relatives à l'administration électronique figurant aux articles 42 et suivants de l'Ordonnance Souveraine n° 3.413 du 29 août 2011.

Il est dénommé « *Portail d'Echange Automatique* » et il est accessible à l'adresse *https://eai.gouv.mc*. Il permet ainsi aux Institutions financières déclarantes, de manière sécurisée, de s'acquitter auprès de la Direction des Services Fiscaux de leurs obligations déclaratives.

La Commission avait relevé que ce projet d'Arrêté Ministériel comportait des dispositions conformes à ses préconisations en matière de collecte et de conservation des documents d'identité, et que les durées de conservation ainsi que les mesures de sécurité de cette plateforme de dépôt répondaient aux exigences en matière de protection des données personnelles.

L'AVIS RELATIF AUX ARRÊTÉS MINISTÉRIELS EN MATIÈRE D'ASSISTANCE ADMINISTRATIVE MUTUELLE EN MATIÈRE FISCALE

Par délibération n° 2018-003 du 17 janvier 2018, la Commission a formulé un avis sur 2 projets d'Arrêtés Ministériels portant application de l'Ordonnance

Souveraine n° 6.208 du 20 décembre 2016 portant application de la Convention concernant l'assistance administrative mutuelle en matière fiscale, de l'Accord multilatéral entre autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers et du Protocole de modification de l'Accord entre la Communauté Européenne et la Principauté de Monaco prévoyant des mesures équivalentes à celles que porte la Directive 2003/48/CE.

A cet égard, elle a eu l'occasion d'analyser la distinction entre les notions de « *juridictions soumises à déclarations* » et « *juridictions partenaires* ».

Aussi, s'agissant des juridictions situées dans des pays ne disposant pas d'un niveau de protection adéquat, elle a rappelé, d'une part, certaines de ses positions de principe, et d'autre part, les dispositions légales attachées à ces communications d'informations.

L'ENCADREMENT DES ÉCHANGES D'INFORMATIONS ENTRE LA CAMTI / CARTI ET LA DIRECTION DE L'EXPANSION ECONOMIQUE

Faisant suite à deux avis défavorables émis en 2016 par la Commission concernant la transmission d'informations entre la CAMTI / CARTI et la Direction de l'Expansion Economique à des fins de vérification de la validité des autorisations d'exercer délivrées aux travailleurs indépendants, le Ministre d'Etat a saisi à deux reprises la Commission au cours de l'année 2018 d'un projet d'Arrêté Ministériel ayant vocation à prévoir et à encadrer la communication d'informations entre ces entités.

En effet lors de ses deux avis défavorables rendus en 2016 la Commission avait considéré que les échanges tels qu'envisagés ne pourraient intervenir « *que si des dispositions conformes à l'ordre public interne répondant aux critères de lisibilité et de prévisibilité les encadraient* ».

Ainsi, par une première délibération en date du 17 janvier 2018 portant avis sur le projet d'Arrêté Ministériel habilitant la Direction de l'Expansion Economique, la CARTI et la CAMTI à échanger les informations nominatives utiles à la gestion des autorisations d'exercer une activité indépendante en Principauté et des procédures d'affiliation auprès des organismes sociaux des travailleurs indépendants , la Commission a relevé que les formulations en projet étaient trop génériques et ne mentionnaient notamment pas l'objectif de ces communications, ainsi que les hypothèses dans lesquelles elles pouvaient avoir lieu.

De même, la nature des informations concernées par ces échanges n'était pas prévue, au même titre que les conséquences pour les travailleurs indépendants de l'absence d'une adresse valide.

Saisie à nouveau du projet d'Arrêté Ministériel modifié pour tenir compte des préoccupations exprimées par la CCIN lors de la saisine initiale par le Ministre d'Etat, la Commission a noté, dans le cadre de sa délibération n° 2018-099 du 18 juillet 2018, que l'essentiel de ses remarques avait effectivement été pris en compte.

Elle a pu constater que l'Arrêté Ministériel n° 2018-905 du 25 septembre 2018 publié suite à ses deux délibérations portant avis sur le texte en projet s'attachait à préciser le cadre de ces échanges d'informations ainsi que les informations pouvant être échangées.

MONACO ET LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

CCIN 8

Le Règlement Général sur la Protection des Données 2016/679 (RGPD ou GDPR, pour *General data protection regulation* en anglais) est le nouveau cadre européen relatif au traitement et à la circulation des données à caractère personnel.

Ce texte, applicable à partir du 25 mai 2018, qui uniformise les législations des Etats membres de l'Union européenne en matière de données personnelles, a vocation à donner à l'ensemble des résidents de l'Union européenne plus de contrôle sur leurs données personnelles, à responsabiliser davantage les responsables de traitements tout en réduisant leurs formalités préalables auprès des régulateurs et à renforcer le rôle des Autorités de protection des données.

Nouveau cadre de référence pour l'Union européenne, c'est à l'aune du RGPD que l'adéquation de la législation monégasque en matière de protection des données personnelles sera examinée.

Cet élément particulièrement important pour les entités monégasques a conduit le Gouvernement Princier à initier une réflexion relative à la modification du droit interne afin d'y intégrer les novations introduites par le RGPD, à laquelle la CCIN a été associée dès l'origine, et qui devrait déboucher sur l'adoption d'une nouvelle législation en 2019 ou au plus tard en 2020.

Bien que pays tiers à l'UE, la Principauté n'en est pas moins impactée par le RGPD dont l'article 3 prévoit, dans certains cas, une extraterritorialité de son application.

Cette portée extra territoriale, et ses impacts pour les entités monégasques concernées, ont conduit la CCIN à multiplier les réunions afin de répondre aux nombreuses questions posées par les responsables de traitement.

De plus, les contours parfois incertains de cette extra territorialité auxquels sont également confrontées les Autorités de Protection des Données de pays se trouvant dans une situation similaire à la Principauté, les ont conduites, de concert avec la CCIN, à interroger le Comité Européen à la Protection des Données sur plusieurs éléments d'importance.

VERS UNE NOUVELLE LOI SUR LA PROTECTION DES DONNÉES PERSONNELLES À MONACO

Le RGPD en plus de renforcer le droit des personnes concernées relativement à leurs informations personnelles, modifie les rapports entre les responsables de traitement et les Autorités de contrôle. Aussi, les responsables de traitement situés sur le territoire de l'Union Européenne n'ont pour une grande majorité plus de formalités préalables à effectuer auprès de leurs régulateurs : c'est le principe de l'accountability, c'est-à-dire que les responsables de traitement doivent pouvoir démontrer qu'ils sont en conformité avec les Lois sur la protection des données personnelles et le RGPD.

A Monaco, le principe de la formalité préalable à la mise en œuvre d'un traitement demeure. Or, le RGPD a une portée extraterritoriale dès lors qu'un responsable de traitement situé à Monaco propose des offres de biens et de services à des personnes se trouvant sur le territoire de l'UE ou qu'il analyse le comportement de telles personnes.

Aussi, un responsable de traitement monégasque peut être soumis au régime de l'accountability et des règles nouvelles du RGPD tout en devant effectuer ses formalités préalables auprès de la CCIN.

Il a donc été estimé nécessaire pour la Place d'offrir les mêmes standards de protection des données qu'en Union européenne et d'harmoniser le régime de responsabilité des sociétés monégasques.

A cet égard, le 7 mai 2018 s'est tenue à l'initiative du Gouvernement deux présentations de Me BENSOUSSAN, l'une pour le secteur privé, l'autre pour le secteur public, afin d'une part d'informer les entités monégasques sur l'extra-territorialité du

RGPD et de ses conséquences, et d'autre part d'indiquer qu'une nouvelle Loi monégasque relative à la protection des données personnelles était en cours d'élaboration, dans la perspective d'une entrée en vigueur en 2019. / 2020. Ainsi, au cours de l'année 2018 de nombreuses réunions avec les Services de l'Etat ont été consacrées à la refonte de la législation monégasque afin d'y introduire les principes structurants du RGPD, tout en les adaptant aux spécificités d'un territoire qui, bien que restreint, comporte un tissu économique dynamique et diversifié.

L'EXTRA TERRITORIALITÉ DU RGPD ET LA COOPÉRATION ENTRE ETATS TIERS À L'UNION EUROPÉENNE

L'article 3 du RGPD étend sous certaines conditions le champ d'application de la législation européenne en matière de protection des données personnelles aux responsables de traitements établis en dehors de celle-ci.

Les pays non membres de l'UE mais géographiquement et économiquement proches de cette dernière, comme c'est le cas de la Principauté, sont particulièrement attentifs aux répercussions que peut avoir le Règlement sur les responsables de traitements situés sur leur territoire.

Partant du principe que les effets du RGPD sont relativement similaires entre leurs pays respectifs et afin d'étudier le spectre le plus large de problématiques qui peuvent se poser à elles, la CCIN échange régulièrement sur ces problématiques avec ses homologues de Suisse, d'Andorre et d'Albanie.

La CCIN et les pays francophones ont également pu faire part de leurs inquiétudes, communes ou spécifiques, lors de la conférence annuelle de l'Association francophone des Autorités de protection des données personnelles qui s'est tenue le 19 octobre 2018 dans les locaux de la CNIL, à Paris.

Le Comité Européen à la Protection des Données a adopté le 16 novembre 2018 des lignes directrices ouvertes à consultation publique, relatives au champ d'application du RGPD, que la CCIN a mises à disposition sur son site.

Dans le cadre d'une démarche conjointe, le Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT) de la Suisse et la CCIN ont participé à cette consultation publique en adressant au Comité Européen à la Protection des Données des remarques et questions sur ces lignes directrices.

Ainsi des demandes de précisions ont porté notamment sur les contours exacts de la notion « *d'offre de biens ou de services* » telle que prévue à l'article 3-2-a du RGPD, sur la problématique des outils statistiques de suivi de comportements sur Internet, ainsi que sur le régime applicable aux transferts d'informations vers des entités situées en dehors de l'Union européenne mais soumises au RGPD compte tenu de sa portée extraterritoriale.

A également été évoquée la question des mécanismes de coopération entre les Autorités de protection des données situées en UE, et celles des pays tiers.

La version définitive de ces Lignes Directrices devrait être publiée dans le courant de l'année 2019.

UNE FOIRE AUX QUESTIONS SUR L'IMPACT DU RGPD EN PRINCIPAUTÉ

Face aux nombreuses interrogations que se posent légitimement les acteurs économiques monégasques sur le RGPD et son application en Principauté, la CCIN a mis en ligne peu avant l'entrée en application du RGPD une foire aux questions (FAQ) afin de présenter les nouvelles obligations pesant désormais sur les responsables de traitement et les sous-traitants, que ce soit en matière de consentement des personnes ou encore de violation de données, ainsi que les principales notions introduites par le texte, telles que le Délégué à la Protection des Données (DPO), l'analyse d'impact ou l' « accountability » .

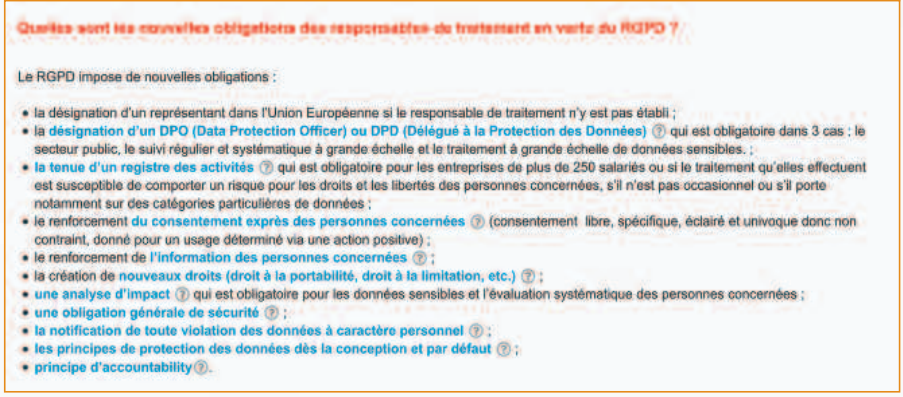
Cette FAQ présente également les sanctions prévues désormais par le texte européen et les principaux droits de la personne concernée qu'il a introduits, comme le droit à l'effacement ou à l'oubli, le droit à la portabilité et le droit à réparation.

Illustrée de cas concrets, comme par exemple celui d'une société monégasque ayant pour objet la vente de produits à des personnes domiciliées en France et en Italie par le biais d'un site de vente en ligne disponible en français et en italien, la FAQ rappelle en outre qu'en plus des obligations prévues par la Loi n°1.165 du 23 décembre 1993, un responsable de traitement ou un sous-traitant peut être aussi soumis aux obligations prévues par le Règlement, en vertu soit du critère d'établissement soit du critère de ciblage, tous deux prévus par l'article 3 dudit texte.

Enfin, elle apporte des éléments de réponse à partir d'exemples précis pour permettre aux responsables de traitement de se conformer au RGPD en listant toute une série d'actions qu'ils peuvent mener, que ce soit faire une cartographie de leurs traitements, effectuer leurs formalités auprès de la CCIN même s'ils sont soumis au RGPD ou encore déterminer s'il est nécessaire pour eux de prendre un représentant dans l'Union européenne.

Cette foire aux questions, intitulée « *Le Règlement Général sur la Protection des Données (RGPD) et son impact à Monaco* », est sur la page d'accueil du site de la CCIN et est régulièrement mise à jour.

https://www.ccin.mc/fr/impact-du-rgpd-a-monaco-faq



Quelles sont les nouvelles obligations des responsables de traitement en vertu du RGPD ?

Le RGPD impose de nouvelles obligations :

- la désignation d'un représentant dans l'Union Européenne si le responsable de traitement n'y est pas établi ;
- la désignation d'un DPO (Data Protection Officer) ou DPD (Délégué à la Protection des Données) qui est obligatoire dans 3 cas : le secteur public, le suivi régulier et systématique à grande échelle et le traitement à grande échelle de données sensibles. ;
- la tenue d'un registre des activités qui est obligatoire pour les entreprises de plus de 250 salariés ou si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur des catégories particulières de données ;
- le renforcement du consentement exprès des personnes concernées (consentement libre, spécifique, éclairé et univoque donc non contraint, donné pour un usage déterminé via une action positive) ;
- le renforcement de l'information des personnes concernées ;
- la création de nouveaux droits (droit à la portabilité, droit à la limitation, etc.) ;
- une analyse d'impact qui est obligatoire pour les données sensibles et l'évaluation systématique des personnes concernées ;
- une obligation générale de sécurité ;
- la notification de toute violation des données à caractère personnel ;
- les principes de protection des données dès la conception et par défaut ;
- principe d'accountability.

SECTEUR PRIVÉ : FOCUS SUR DES PROBLÉMATIQUES SPÉCIFIQUES

CCIN 9

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 2018.

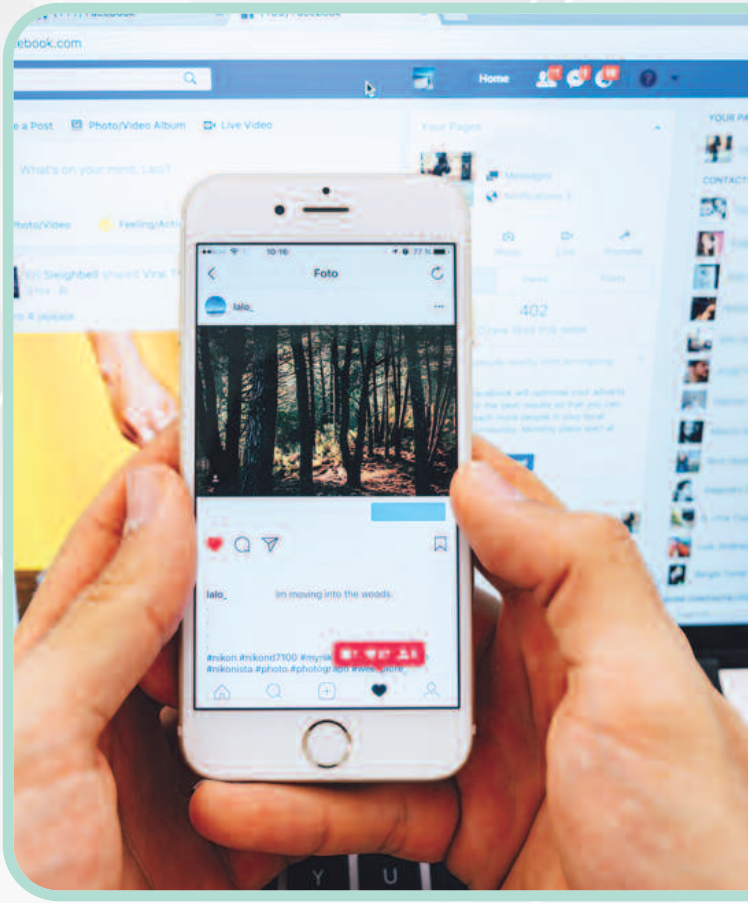
L'UTILISATION DE FACEBOOK CONNECT SUR UN SITE INTERNET

Quel utilisateur Facebook ne s'est pas laissé tenter par cette application qui permet en un seul clic de créer un compte sur de nombreux sites sans avoir à passer de longues minutes à remplir des formulaires parfois interminables ? De même, comment résister à la case "Se souvenir de moi" qui, si elle est cochée, permet ensuite d'être connecté automatiquement à tous ses sites préférés sans aucun effort ? Rapide, simple et efficace.

Mais si Facebook Connect présente des avantages pour un utilisateur pressé, il comporte toutefois un risque certain pour ses données personnelles. En effet, sans que cet utilisateur en ait nécessairement conscience, le célèbre réseau social transmet au site visité toutes les données publiques du profil dudit utilisateur. C'est ainsi que des informations de base telles que son nom complet, son âge, son sexe, sa liste d'amis ou encore ses intérêts ou ses mentions « *j'aime* » sont susceptibles d'être immédiatement communiquées au site tiers.

Heureusement, l'utilisation de Facebook Connect ne permet pas au site utilisant la fonction de devenir propriétaire des données identifiantes des utilisateurs et donc de les traiter ultérieurement. Toutefois, ces opérateurs peuvent recevoir bien plus de données sur leurs utilisateurs qu'ils n'arriveraient à en rassembler, en général, lors d'une inscription normale par le biais de leurs formulaires.

Quelles conséquences pour les responsables de sites internet utilisant Facebook Connect ?



Puisque ces responsables collectent des informations personnelles par le biais de cette application, ils doivent indiquer l'utilisation de ladite application lorsqu'ils déclarent, par le biais d'une déclaration ordinaire, leur site internet auprès de la Commission. Ainsi dans la rubrique « *fonctionnalités du traitement* », de même qu'ils indiquent « *création d'un compte client par le biais d'un formulaire d'inscription* », il doivent également ajouter « utilisation de Facebook Connect pour créer un compte ». De la même manière, ils doivent préciser dans la rubrique « *Autres données traitées* », toutes les informations qu'ils collectent par le biais de cette application ainsi que leur durée de conservation.

Quels conseils pour les visiteurs d'un site qui utilise Facebook Connect ?

Il est recommandé à tout utilisateur ne souhaitant pas que les informations qu'il a communiquées à Facebook soient transmises au site qu'il visite, de prendre les précautions suivantes :

- Privilégier une création de compte par adresse email plutôt qu'une connexion automatique, pour limiter la collecte de données et désamorcer à son échelle leur commerce.

- Changer régulièrement de pseudo/identifiant, pour endiguer le croisement de données, l'augmentation de leur valeur et donc de leur trafic.

- Créer un compte Facebook « fantôme », pour utiliser la connexion automatique.

- Envisager de désactiver Facebook Connect sur son compte personnel, pour éviter tout problème.

DÉTERMINATION DES FORMALITÉS LIÉES AUX SYSTÈMES D'INFORMATION EN FONCTION DE LA NOTION DE CONTRÔLE OU DE SURVEILLANCE

La mise en place d'un véritable système d'habilitation au sein d'une entreprise ou d'un organisme est aujourd'hui essentielle afin de sécuriser les systèmes d'information (SI) et de garantir la confidentialité des données que celui-ci contient.

Ce système va permettre au responsable de traitement de s'assurer que chaque utilisateur du SI n'a accès **qu'aux seules données** dont il a besoin pour l'exercice de sa mission, ce qui se traduit au niveau interne par la nécessaire définition des niveaux d'habilitation d'un utilisateur dans le système, et d'un moyen de contrôle des permissions d'accès aux données.

Pour cela, le responsable de traitement doit notamment déterminer au préalable :

- les données et applications auxquelles ledit utilisateur peut avoir accès, de manière dédiée ou partagée (réseau local ou partagé, dossiers de travail, imprimantes, téléphones, etc.) ;

- l'étendue des droits ainsi conférés : accès en simple consultation, en inscription, en suppression.

Par ailleurs, la mise en place de ce système impliquant la collecte d'informations nominatives, le traitement automatisé y afférant est soumis aux formalités prévues par la Loi n° 1.165 du 23 décembre 1993.

Ces formalités seront toutefois différentes selon que lesdites habilitations sont mises en œuvre à des fins de surveillance ou non. Dans le premier cas, le responsable de traitement devra soumettre à la Commission une demande d'autorisation préalable, conformément à l'article 11-1 de la Loi n°1.165 du 23 décembre 1993 alors que dans le second cas, une déclaration simplifiée devra être déposée, conformément à l'Arrêté Ministériel n°2016-501 du 5 août 2016 relatif aux modalités de déclaration simplifiée des traitements automatisés d'informations nominatives relatifs à la gestion administrative des salariés.

En pratique, cette notion de contrôle ou de surveillance est toutefois souvent bien difficile à appréhender par les responsables de traitements. C'est pourquoi, la Commission a précisé dans sa recommandation n° 2017-206 du 20 décembre 2017 sur les traitements automatisés d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* » que cette notion de contrôle ou de surveillance du système de gestion des habilitations devait se concevoir comme « ***toute activité qui consiste en la collecte, la détection et/ou l'enregistrement, dans le cadre de rapports établis à intervalles réguliers, des données à caractère personnel d'une ou de plusieurs personnes, relatives à l'utilisation des habilitations informatiques*** ».

A titre d'exemple, elle considère ainsi que cette définition peut inclure la supervision par le biais d'un système de remontée d'alerte et/ou d'alarme. La Commission a par ailleurs profité de cette recommandation pour rappeler les grands principes en matière d'habilitations informatiques que

les responsables de traitement doivent avoir en tête avant de mettre en place leurs systèmes d'habilitations. Ces principes sont au nombre de deux :

Des profils d'habilitation définis, formalisés et auditables

Pour la Commission, il est nécessaire pour toutes les catégories de comptes (nominatifs ou collectifs), d'identifier et d'authentifier tout utilisateur en fonction notamment du niveau de risque associé à la ressource, du type d'utilisateur ou encore du type d'accès. Cette séparation des tâches et des domaines de responsabilité permet ainsi de limiter l'accès à des données à caractère personnel aux seuls utilisateurs dûment habilités.

A cet égard, elle demande au responsable de traitement de respecter d'une part le principe du « *besoin d'en connaître* » qui correspond à la définition, par le métier, des habilitations nécessaires pour l'activité d'un utilisateur donné, et d'autre part le principe « *du moindre privilège* » qui consiste à mettre en place les habilitations strictement nécessaires aux activités liées à chaque compte.

La Commission demande également que les modalités d'octroi des habilitations soient documentées et rappelle que les permissions d'accès des utilisateurs doivent être supprimées ou modifiées dès lors que ces derniers ne sont plus habilités à accéder à une ressource car ils ont quitté l'entité ou bien changé de fonctions.

Enfin, elle demande aux propriétaires du système d'information de vérifier régulièrement la pertinence des profils et des accès accordés.

Une politique de validation des habilitations et de gestion des mobilités

Pour la Commission, il est très important que toute demande d'habilitation soit validée au moins par le responsable hiérarchique de la personne à habiliter. Par ailleurs, même si ledit responsable délègue cette tâche, celui-ci doit nécessairement conserver la responsabilité des habilitations de son équipe et de celles attribuées aux personnes effectuant des prestations de service pour son compte.

La Commission demande également au responsable de traitement de veiller à la gestion efficace de tout changement de poste ou de départ afin d'éviter l'accumulation des habilitations. Ainsi lorsqu'une personne est mutée ou quitte l'entité, les habilitations dont elle disposait doivent être modifiées ou retirées immédiatement.

Pour plus d'information sur le sujet, la délibération n° 2017-206 du 20 décembre 2017 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* » est disponible sur le site internet de la Commission.

LA SÉCURITÉ DES DONNÉES PERSONNELLES DANS LE CLOUD

Terme désormais très répandu mais souvent encore méconnu, le « *Cloud computing* » désigne le déplacement des traitements et fichiers informatiques de l'ordinateur local vers des serveurs distants. Appelé également en français « *l'informatique en nuage* » il permet d'exploiter des logiciels en ligne, d'archiver ses données, d'utiliser une puissance de calcul mutualisée, et de collaborer au sein d'espaces virtuels partagés.

C'est ainsi par exemple que chaque personne peut maintenant consulter ses emails en ligne, en tapant simplement l'adresse de son webmail

(Yahoo Mail, Hotmail, GMail, etc.) sur n'importe quel ordinateur puis en s'identifiant. Elle accède alors à une interface web et un espace virtuel de stockage (messages, pièces jointes, etc.).

De même, beaucoup de personnes utilisent aujourd'hui Dropbox pour stocker, sauvegarder et partager des documents en ligne.

Les avantages de « *ce nuage* » sont nombreux pour les entreprises puisqu'il permet notamment :

- **la réduction des coûts :** la mutualisation des ressources informatiques et la facturation à l'usage rend le « *Cloud Computing* » économiquement attrayant ;
- **l'accessibilité :** les services de « *Cloud Computing* » sont accessibles à tout moment, sur tous les supports, via une connexion internet ;
- **le déploiement rapide et la simplicité d'intégration :** le déploiement et la mise en fonctionnement d'un service de « *Cloud Computing* » nécessite peu de temps ;
- **la disponibilité du service :** le « *Cloud Computing* » permet de garantir les accès et la disponibilité des services. Le fournisseur de services de « *Cloud Computing* » s'engage contractuellement sur une interruption minimum des serveurs à travers des SLA (service Level Agreements) ;
- **la protection de l'environnement :** le « *Cloud Computing* », basé sur la virtualisation de serveurs, la mutualisation de la puissance de calcul et la flexibilité des services s'inscrit dans une démarche éco-responsable ;
- **la réversibilité :** la restitution de l'intégralité des données d'une entreprise est garantie par les fournisseurs prévoyant dans leur contrat une clause de réversibilité.

Toutefois, malgré tous ces bénéfices, l' « *informatique en nuage* » possède quelques défauts et comporte certains risques, notamment au niveau de la sécurité et la protection des données stockées.

En effet, la plateforme cloud, si elle est externe (non installée sur le réseau interne ou avec une ouverture extérieure) doit être suffisamment sécurisée pour éviter le risque d'intrusion ou de vol des données par piratage. L'autre risque est qu'un utilisateur oublie de se déconnecter sur un appareil accessible par des éléments externes à l'organisation.

Il est donc très important qu'un responsable de traitement ayant recours à un service d' « *informatique en nuage* » prenne les mesures suivantes afin d'assurer la sécurité des données qu'il transmet :

1. **Une stratégie interne de sécurisation :** tout responsable de traitement doit impérativement bien segmenter les droits utilisateurs afin que ces derniers ne puissent accéder qu'aux données des projets dans lesquels ils sont impliqués. Une procédure d'identification efficace (mots de passe complexes et différents pour chaque utilisateur, etc.) doit également être déployée Par ailleurs, des sauvegardes régulières doivent être effectuées et un firewall ainsi qu'un antivirus doivent être installés.

2. **La localisation et la disponibilité des données :** il est indispensable, lorsque l'on confie des données à un tiers, de savoir où celles-ci sont stockées. En effet, les risques juridiques varient selon les pays, et les garanties sur la protection des données diffèrent dans et hors de l'Union Européenne. En outre, la localisation des données doit être suffisamment proche pour minimiser la latence due à l'éloignement dans le réseau en fonction des exigences du système d'information du client.

3. **Le choix du fournisseur :** tout fournisseur de Cloud doit être entièrement conforme aux dernières normes de sécurité et doit disposer des certifications largement admises dans le secteur, y compris les obligations réglementaires spécifiques applicables à l'entreprise cliente. Il est vital en effet que le fournisseur suive les bonnes pratiques afin de prévenir toutes les menaces futures.

4. **La validation de la compétence de son prestataire :** il est nécessaire de vérifier des éléments comme la réputation du fournisseur, les normes et labels que celui-ci a obtenus, ou encore les publications de ses experts maison. La norme ISO 27001 valide le fait que l'entreprise a mis en œuvre les mesures nécessaires pour éviter la perte, le vol ou l'altération de ses données.

5. **La confiance :** il faut aussi exiger de son fournisseur des documents contractuels particuliers et investir dans des audits pour vérifier sa fiabilité.

L'ÉVOLUTION DES TRAITEMENTS DE GESTION DES ALERTES PROFESSIONNELLES

La Commission avait pris position sur les alertes professionnelles le 26 septembre 2011 en adoptant une délibération portant recommandation sur le

sujet. A ce titre, elle estimait que de tels traitements pouvaient être « *mis en œuvre aux seules fins de :*

- *répondre à une obligation législative ou réglementaire de droit monégasque visant à l'établissement de procédures de contrôle interne dans les domaines financier, comptable, bancaire et de lutte contre la corruption ; ou –*
- *permettre la réalisation d'un intérêt légitime poursuivi par le responsable de traitement ou son représentant, à la condition de ne pas méconnaître les libertés et droits fondamentaux des personnes concernées.*

Sont ainsi justifiés les traitements d'alerte professionnelle mis en œuvre dans les domaines :

- *comptable et d'audit, notamment par les entreprises ou organismes concernés par la section 301(4) de la loi américaine dite « Sarbanes-Oxley » du 31 juillet 2002, ou par la loi japonaise « Financial Instrument and Exchange Act » dite « Japanese SOX » du 6 juin 2006 ;*
- *de lutte contre les pratiques anticoncurrentielles.*

Aussi, soucieuse de respecter le cadre défini dans la recommandation afin que les alertes professionnelles ne servent pas à toutes finalités, la Commission a été amenée à refuser ou amender des traitements présentant un spectre trop important.

Toutefois, elle a révisé sa position suite à l'adoption à Monaco de la Loi n° 1.457 du 12 décembre 2017 relative au harcèlement et à la violence au travail, aux termes de laquelle « *(...)[l'employeur] met en place des procédures appropriées destinées à prévenir de tels faits et, le cas échéant, les identifier et y mettre un terme. (...)* ».

Aussi les autorisations de mise en œuvre qu'elle délivre depuis s'inscrivent dans ce périmètre ainsi élargi.

CCIN 10

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

Journée de présentation du RGPD

La CCIN a assisté le 7 mai 2018 à la journée d'information organisée à l'initiative du Gouvernement Princier et animée par Me Alain Bensoussan, avocat spécialisé en droit des nouvelles technologies, sur la mise en place du Règlement Général sur la Protection des Données et sur ses enjeux et impacts en Principauté.

Destinée à la fois aux acteurs privés lors de la session du matin et au secteur public lors de la session de l'après-midi, cet évènement a été l'occasion de présenter les nouveaux droits et obligations prévus par ledit Règlement et de rappeler qu'un responsable de traitement ou sous-traitant situé à Monaco pourra dans certaines circonstances être impacté par ce texte.

Les interrogations qu'a suscitées cette présentation ont conduit de nombreux responsables de traitement à se rapprocher de la CCIN afin d'obtenir des clarifications sur certains éléments évoqués, dont notamment les contours exacts de l'extraterritorialité du RGPD.

Sensibilisation des futurs infirmiers à la protection des données de santé

Le 9 mai 2018 deux agents du Secrétariat se sont rendus à l'Institut de Formation en Soins Infirmiers afin de présenter la CCIN mais aussi de sensibiliser les futurs infirmiers aux problématiques de la protection des données nominatives dans le domaine de la santé. L'accent a ainsi été mis sur la nécessité d'obtenir le consentement libre et éclairé du patient avant tout acte médical et sur les modalités d'information telles que désormais prévues en Principauté en vertu de la Loi n°1.454 du 30 octobre 2017 et de l'Ordonnance Souveraine n° 6.903 du 27 avril 2018. Le cas particulier des mineurs a par ailleurs été souligné et les mesures à prendre pour sécuriser les données de santé ont été détaillées.

Participation à la 18ème édition des Assises de la Sécurité

Devenues l'évènement phare de la rentrée dans le domaine de la sécurité informatique, les Assises de la Sécurité et des systèmes d'informations, dont la 18ème édition s'est déroulée du 10 au 13 octobre 2018 au Grimaldi Forum, témoignent de l'ancrage pris par le secteur de l'informatique et des technologies matures dans la Principauté, permettant de réunir les plus éminents professionnels, acteurs, dirigeants internationaux, parlementaires et autres experts en la matière au sein du territoire monégasque.

Au fil des multiples conférences, keynotes, one-to-one, ateliers et autres tables rondes, la CCIN a eu l'occasion d'échanger durant ces quatre journées

avec les spécialistes et techniciens de la cybersécurité, et ainsi d'évoquer les innovations relatives au risque numérique et à la cybermenace : nouveaux moyens mis en œuvre permettant de transférer avec plus de visibilité et de contrôle les données numériques vers le Cloud, la transformation digitale au sein des entités administratives, l'influence croissante du secteur de la robotique, les nouvelles méthodologies en matière d'analyse de code, la protection de l'identité des machines, l'usage de la *threat intelligence*, l'optimisation de la détection des menaces avancées, ou encore les conséquences pratiques de l'application par diverses entreprises du RGPD d'un point de vue organisationnel et fonctionnel.

La Journée d'information de l'AFCDP à Nice

Le 23 novembre, un agent de la CCIN s'est rendu à la journée d'information organisée par l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP) qui s'est tenue à la Chambre de Commerce et de l'Industrie de Nice.

Destinée aux entreprises, cette conférence avait pour but principal de dresser un tableau des enjeux de la mise en conformité au RGPD grâce à des ateliers de 45 minutes animés par des experts.

De nombreux sujets tels que les mentions d'information obligatoires, le consentement des personnes concernées et la responsabilité conjointe entre responsables de traitement et sous-traitants ont ainsi été au centre des discussions.

Par ailleurs, Matthieu GRALL, Chef du service de l'expertise technologique à la CNIL a évoqué les aspects sécurité du RGPD et Adrienne CHARMET, Chargée de mission Relations institutionnelles, au sein du GIP ACYMA, a présenté « *Cybermalveillance.gouv.fr* », le programme mis en place par le Gouvernement français afin d'assurer un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population .

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

Renforcement de la coopération entre les Autorités monégasque et malienne

Dans le cadre de la coopération entre les Autorités francophones de protection des données personnelles, la Commission de Contrôle des Informations Nominatives a accueilli, courant février 2018, le Chef de Division des Affaires Juridiques au sein de l'Autorité malienne de protection des données à caractère personnel (l'APDP) pour une visite de travail de 10 jours. Une occasion pour ces deux Autorités d'échanger sur leurs expériences respectives, de

partager leurs préoccupations et leurs réalisations mais surtout de se rendre compte que malgré les différences culturelles, les problématiques rencontrées dans leur activité quotidienne sont les mêmes.

Monsieur HAIDARA entouré des Agents du Secrétariat Général

Monsieur HAIDARA s'est notamment montré particulièrement intéressé par les recommandations rédigées par l'Autorité monégasque dans les domaines de la vidéosurveillance, de la messagerie électronique, des enregistrements téléphoniques, de la règlementation FATCA , de la géolocalisation, de la gestion administrative des salariés, de la gestion des habilitations et des accès au système d'informations, de la gestion du contentieux et de la gestion des dispositifs de contrôle d'accès que ce soit par le biais de badges magnétiques ou par le bais de la biométrie.

Il a également pris connaissance des brochures, rapports d'activité et guides pratiques publiés par la CCIN, plus particulièrement dans le domaine de la sécurité des fichiers et de la protection des données numérisées.

Monsieur HAIDARA a par ailleurs pu observer les différentes formalités à accomplir en Principauté ainsi que les différentes étapes de l'instruction des dossiers, de leur dépôt par les responsables de traitement jusqu'à leur passage en Commission, pour les dossiers soumis à autorisation ou à avis préalable.

Enfin, il a eu l'occasion de rencontrer l'équipe technique de la CCIN en charge des outils métiers permettant l'accomplissement des formalités en ligne.

L'Autorité du Mali est une Autorité de contrôle récente (créée par la Loi n°2013-015 du 21 mai 2013) qui a officiellement commencé ses activités en mars 2015 et qui est très à l'écoute de ce qui se passe chez ses consœurs francophones. L'exemple de Monaco est une source d'inspiration pour elle et grâce à cette visite, des liens ont pu être créés entre les deux Autorités afin de collaborer de façon plus étroite dans le futur, notamment à l'aune de l'entrée en vigueur du nouveau Règlement européen qui aura un impact pour la Principauté de Monaco mais également pour le continent africain.

Participation à la Conférence de printemps des Autorités européennes de protection des données à caractère personnel

Les 3 et 4 mai 2018, deux agents du Secrétariat se sont rendus à Tirana afin d'assister à la 28ème édition de la Conférence des Autorités européennes de protection des données à caractère personnel (DPA) organisée pour la première fois dans la région des Balkans autour du thème « *Data Protection – Better Together* ».

A quelques jours seulement de son entrée en application, le Règlement Général sur la Protection des Données a été au centre des discussions avec notamment une session consacrée à la portée territoriale de ce texte et ses conséquences pour les pays tiers à l'Union européenne, ainsi qu'une session dédiée au rôle et au renforcement de la coopération des Autorités de protection des Données dans la supervision des agences de surveillance.

Les questions de la protection des données à caractère personnel dans le contexte de la police et des institutions judiciaires, l'influence des normes européennes et la protection des données dans les actions humanitaires ont également fait l'objet de plusieurs exposés, tandis qu'un autre sujet d'actualité particulièrement brûlant, suite au scandale Cambridge Analytica, a donné lieu à une session particulière consacrée aux médias sociaux, au micro-ciblage et aux campagnes politiques.

Par ailleurs, les travaux en cours de la Commission européenne relatifs à l'efficacité de la justice en ce qui concerne l'utilisation de l'intelligence artificielle dans le cadre de la justice ainsi que ceux menés pour la modernisation de la Convention 108 du Conseil de l'Europe (« Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ») ont été présentés.

Enfin, les participants se sont penchés sur le document préparé par le Groupe de travail sur l'avenir de la Conférence, comprenant 12 Autorités de protection des données, dont la CCIN. Il a été proposé de prolonger d'un an le mandat de ce groupe de travail afin que celui-ci puisse poursuivre ses réflexions et proposer l'année prochaine de nouvelles règles de fonctionnement.

12ème Assemblée générale de l'AFAPDP à Paris

ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES

Les 18 et 19 octobre, la CCIN s'est rendue à l'invitation de la Commission Nationale de l'Informatique et des Libertés de France (CNIL) à la 12ème Assemblée générale de l'Association francophone des Autorités de protection des données personnelles (AFAPDP).

Organisé à Paris avec le soutien de l'Organisation Internationale de la Francophonie (OIF), ce rassemblement a été l'occasion pour les délégations présentes de se pencher sur la question de la « *patrimonialisation des données personnelles* » avec l'adoption d'une résolution rappelant que « *les données à caractère personnel sont des éléments constitutifs de la personne humaine qui dispose, dès lors, de droits inaliénables sur celles-ci* ».

Pour les Autorités francophones, il est en effet important de créer les conditions d'une relation

contractuelle équitable entre les personnes dont les données sont collectées et les responsables de traitement.

Des échanges nourris ont par ailleurs eu lieu sur les nouvelles pratiques électorales ainsi que sur la manipulation de l'information et la propagation de fausses nouvelles sur les réseaux sociaux.

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 que de promouvoir l'établissement d'un réseau d'échange et de coopération entre les Autorités indépendantes chargées de la protection des données.

Elle compte désormais 20 membres depuis l'adhésion du Cap-Vert à l'occasion de cette Assemblée générale.

40ème Conférence internationale des commissaires à la protection des données et de la vie privée à Bruxelles

Du 22 au 26 octobre, la CCIN a participé à la 40ème Conférence internationale des commissaires de la protection des données et de la vie privée, organisée à Bruxelles sous l'égide du Contrôleur Européen à la Protection des Données (CEPD), autour du thème « *Debating Ethics : Dignity and respect in data driven life* ».

Lors des deux premiers jours, la session fermée de la Conférence a donné l'occasion aux commissaires de plus de 70 délégations de réfléchir ensemble sur la révolution numérique et son impact sur nos sociétés, ainsi que sur la façon dont une nouvelle éthique numérique pourrait contribuer à garantir le respect et la dignité dans notre monde dominé par la technologie.

En effet, comme l'a souligné Madame Isabelle Falque-Pierrotin, Présidente de la CNIL et Présidente de la Conférence Internationale dans son discours d'ouverture, ces sujets « *ont pris une dimension nouvelle et ils s'étendent à de nouvelles problématiques, plus politiques, plus éthiques. Ils se manifestent dans un environnement international qui, s'il n'a jamais été paisible, est aujourd'hui*

particulièrement contrasté. D'un côté, les tensions sont là, et ce y compris sur des questions qui sont au cœur de notre mission comme la localisation des données, la cyber-sécurité ou encore la surveillance de masse et les techniques de renseignement » et « *De l'autre, le numérique est une opportunité de développement unique au niveau mondial, une véritable révolution. « Tech for good*» ou « *AI for humanity* » *sont désormais à l'agenda des réunions de nos chefs d'état et de gouvernement et le potentiel de ces technologies pour trouver des solutions pour l'humanité est immense* ».

A l'issue de ces deux jours, une déclaration sur la protection des données et l'éthique dans le domaine de l'intelligence artificielle et 5 résolutions ont été adoptées. Ces dernières portent sur :

- les plateformes d'e-learning ;
- la modification des règles et procédures concernant la Conférence internationale ;
- la feuille de route sur l'avenir la Conférence internationale ;
- la collaboration entre les Autorités de protection des données et les Autorités de protection des consommateurs ;
- le recensement concernant les Conférences internationales.

Cette session fermée s'est poursuivie par une session ouverte organisée au Parlement européen qui a permis aux acteurs de la société civile de prendre part au débat. Parmi toutes les prises de parole, on retiendra notamment celle de Tim Cook, le dirigeant d'Apple qui a profité de l'occasion pour dire tout le bien qu'il pensait du RGPD mis en œuvre en Europe, et demander à ce qu'une réglementation similaire soit adoptée aux États-Unis.

64ème réunion de l'IWGDPT et 50ème forum de l'APPA en Nouvelle-Zélande

Fin novembre, deux agents du Secrétariat se sont rendus en Nouvelle-Zélande pour assister à la 64ème réunion du groupe de travail IWGDPT, puis, à l'invitation de John Edwards, Commissaire à la Vie Privée, au 50ème Forum des Autorités de protection de la vie privée de la zone Asie-Pacifique (APPA : Asia Pacific Privacy Authorities).

Plus connu sous le nom de « *Groupe de Berlin* », l'IWGDPT réunit deux fois par an des Autorités de protection de la vie privée, des administrations et des organisations venant des 4 coins de la planète afin de fournir à ses membres et au public des documents de travail sur des évolutions technologiques spécifiques et leur incidence sur la protection de la vie privée et des données.

A Queenstown, les discussions ont notamment porté sur la protection des enfants sur les réseaux sociaux, les jouets intelligents et la portabilité des

données. Elles ont par ailleurs abouti à l'adoption de deux documents, le premier sur la vie privée et l'Intelligence Artificielle, et le deuxième sur la géolocalisation à grande échelle.

Enfin, Peter Fleischer, responsable de la protection des données chez Google, et Laura Juanes, responsable de la politique de confidentialité chez Facebook ont été invités à présenter les mesures prises par leurs entreprises respectives suite à l'adoption du Règlement Général sur la Protection des Données.

Ces mêmes sujets ont également été évoqués la semaine suivante à Wellington, lors du forum annuel de l'APPA.

Même à l'autre bout de la terre, le RGPD a suscité la curiosité des participants, avec une présentation du texte, 6 mois après son application, par Elizabeth Denham, Commissaire britannique à l'Information.

Contribution à la traduction du nouveau Manuel de droit européen en matière de protection des données

En 2017 la CCIN avait participé à la finalisation de la version anglaise du nouveau Manuel de droit européen en matière de protection des données, édité par l'Agence des droits fondamentaux de l'Union européenne et le Conseil de l'Europe.

L'année 2018 a été pour elle l'occasion de procéder à une relecture de la version française de ce manuel mis à jour afin d'y intégrer les dispositions du RGPD, de la Convention 108 modernisée, et les références à des jurisprudences récentes.

Ce manuel est accessible depuis le site Internet de la CCIN.

PERSPECTIVES 2019

CCIN 11

Dans le prolongement des travaux initiés en 2018 avec les Services de l'Etat, la Commission poursuivra ses réflexions relatives à la modification structurelle de la législation interne régissant la protection des informations nominatives afin d'y intégrer les principes désormais inscrits dans le RGPD, applicable depuis le 25 mai 2018 sur le territoire de l'Union européenne.

A cet égard la CCIN aura bien évidemment à l'esprit le nouveau référentiel d'adéquation publié en toute fin d'année 2017 par le Groupe de travail européen des autorités de protection des données personnelles (devenu le Comité européen de la protection des données depuis le 25 mai 2018), lequel définit le « *noyau dur des principes de protection des données qui doivent être garantis par le cadre juridique d'un pays tiers (...) afin d'assurer l'équivalence nécessaire avec le cadre européen.* »

En effet la modification du droit interne a une double vocation : tout à la fois aligner la législation monégasque sur les plus hauts standards internationaux régissant la protection des données personnelles, et obtenir de la part de l'Union européenne la reconnaissance du niveau de protection adéquat de la législation monégasque, afin d'assouplir les modalités de transfert des données à caractère personnel en Principauté, et ainsi de fluidifier, dans un environnement protecteur, la circulation des données.

L'année 2019 devrait être marquée par la publication de la version définitive des « *Lignes directrices* » établies par le Comité européen à la protection de la protection des données, relatives à la portée extraterritoriale du RGPG, sur lesquelles la CCIN et l'Autorité de protection des données de la Suisse ont fait part conjointement de leurs remarques dans le cadre de la consultation publique ouverte en fin d'année 2018.

Compte tenu des enjeux liés, pour les entités publiques et privées de la Principauté, à la soumission de certains de leurs traitements au Règlement européen, la CCIN et son homologue suisse se sont en effet attachés à tenter d'obtenir des précisions sur les contours exacts de cette extraterritorialité afin que la version définitive des « *Lignes directrices* » éclaircisse les zones d'ombre de l'article 3 du RGPD.

Par ailleurs, compte tenu du nombre sans cesse croissant de responsables de traitements qui utilisent sur leur site Internet des outils statistiques de mesure d'audience et d'analyse de comportement, dont certains transfèrent les données nominatives des internautes vers un pays ne disposant pas d'un niveau de protection adéquat, la CCIN adoptera en 2019 une Recommandation destinée à encadrer le recours à ces « *traceurs* ».

En outre, afin de préciser les grands principes applicables aux mesures de sécurité qui doivent entourer les cartes de paiement en matière de vente de biens ou de fourniture de services à distance, ainsi que les sites web présentant cette possibilité, la Commission adoptera également une Recommandation sur ce point.

Ces deux Recommandations s'inscrivent dans le cadre de la modification prochaine de l'Arrêté Ministériel n° 2010-191 du 7 avril 2010 relatif aux modalités de déclaration simplifiée de conformité des traitements automatisés d'informations nominatives portant sur la gestion des fichiers de clients et de prospects.

En effet, en l'état actuel de ce texte, les activités de vente par correspondance ne sont pas éligibles à cette déclaration simplifiée. L'objectif est donc d'ouvrir la vente à distance à cette formalité simplifiée, tout en l'encadrant par le bais de ces Recommandations.

L'année 2019 marquera également la fin de mandat des Commissaires dont la nomination est intervenue au mois de juin 2014.

Dans le droit fil des travaux entrepris au cours du mandat qui va s'achever, la Commission nouvellement nommée aura, sans aucun doute, la volonté de poursuivre le dialogue étroit et constructif noué 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.

FICHES PRATIQUES

CCIN 12

LA CYBER SURVEILLANCE AU TRAVAIL

L'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution énoncent le principe fondamental du droit au respect de la vie privée et familiale de toute personne, droit qui s'étend également au monde du travail selon la jurisprudence de la Cour européenne des droits de l'homme (CEDH).

En effet, dans son arrêt, *Niemietz c. Allemagne*, la Cour a considéré « *qu'il serait trop restrictif de limiter (la vie privée) à un cercle intime où chacun peut mener sa vie personnelle à sa guise et* ***d'en écarter entièrement le monde extérieur à ce cercle.*** *Le respect de la vie privée doit aussi englober dans une certaine mesure le droit de l'individu de nouer et de développer des relations avec ses semblables... Il n'y a aucune raison de principe d'en exclure les activités professionnelles ou commerciales* ».

Si le droit au respect de la vie privée et au secret des correspondances s'étend aujourd'hui au lieu de travail, ce droit dont jouissent les employés est néanmoins susceptible de connaître des limitations justifiées par le respect d'intérêts légitimes de l'employeur.

En effet, pour des raisons de sécurité notamment, ce dernier peut être amené de manière directe ou indirecte à contrôler ses salariés, grâce à des dispositifs allant de la consultation de la messagerie électronique et de l'enregistrement des conversations téléphoniques à la vidéosurveillance, la géolocalisation ou encore le contrôle des accès aux locaux.

Entrent alors en conflit deux intérêts apparemment contradictoires, mais néanmoins conciliables, entre lesquels il convient de trouver un juste équilibre.

Cette fiche pratique a donc vocation à résumer les droits et obligations des employeurs vis-à-vis de leurs employés lors de la mise en place de dispositifs de surveillance sur le lieu de travail.

La messagerie professionnelle

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

➢ *Fonctionnalités autorisées*

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

- échange de messages électroniques en interne ou avec l'extérieur ;
- historisation des messages électroniques entrants et sortants ;
- gestion des contacts de la messagerie électronique ;
- gestion des dossiers de la messagerie et des messages archivés ;
- établissement et lecture de fichiers journaux ;
- gestion des habilitations d'accès à la messagerie ;
- gestion de l'agenda ;
- mise en place d'une procédure de contrôle gradué ;

- contrôle au moyen d'un logiciel d'analyse du contenu des messages électroniques entrants ou sortants ;

- établissement de preuves en cas de litige avec un client/employé (en cas de contestation d'un ordre, etc..).

➢ **Protection des correspondances privées sur le lieu de travail**

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

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

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

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

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

➢ ***Dispositions en cas d'absence ou de départ de l'employé***

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

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

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

En outre, en cas de départ définitif de l'entreprise, l'employeur devra avertir l'employé de la date de fermeture de son compte afin de lui permettre de vider sa messagerie de ses messages personnels. Il devra également supprimer l'adresse électronique nominative de l'employé 3 mois maximum après le départ dudit employé.

➢ ***Modalités d'information des utilisateurs***

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

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

➢ ***Modalités d'information des tiers destinataires***

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

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

➢ ***Durée de conservation des données***

Conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, les informations nominatives objets du traitement ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont exploitées.

Ainsi, la Commission demande à l'employeur de prévoir les durées de conservation de données suivantes :

- s'agissant de l'administration de la messagerie électronique (compte individuel et carnet d'adresses) : 3 mois maximum après le départ de l'utilisateur ;
- s'agissant du contenu des messages émis et reçus, la Commission demande qu'une politique d'archivage soit mise en place jusqu'à ce que la conservation desdits messages ne soit plus nécessaire ;

- s'agissant des données de connexion (logs, horodatage, fichiers journaux....) : 1 an maximum, en fonction de l'activité exercée.

En tout état de cause, la Commission recommande, lorsque cela est possible, d'adopter une durée de conservation moindre, dès lors que les données traitées ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été initialement collectées, conformément à l'article 10-1 susvisé.

Les dispositifs d'enregistrement des conversations téléphoniques

La mise en place de dispositifs d'enregistrements téléphoniques comprend un certain nombre de dangers intrinsèques, et notamment :

- le risque d'atteinte à la vie privée des employés lors d'une utilisation à caractère privé du téléphone ;
- le risque de disproportion entre le dispositif mis en place et les objectifs poursuivis par l'employeur ;
- la déloyauté de la collecte et du traitement des données nominatives d'une personne n'ayant pas les moyens de s'y opposer ou de se défendre.

➢ ***Fonctionnalités autorisées***

La Commission estime que des dispositifs d'enregistrements téléphoniques peuvent être mis en place pour les finalités suivantes :

- la traçabilité des ordres ;
- le contrôle de la régularité des opérations financières et bancaires effectuées dans le cadre de l'obligation de vigilance ;
- le contrôle qualité par échantillonnage et de manière aléatoire ;
- la résolution des malentendus ;
- l'établissement de preuves en cas de litige.

➢ ***Garanties pour la vie privée des salariés***

La Recommandation CM/Rec(2015)5 du Conseil de l'Europe du 1er avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi précise que « *le respect de la dignité humaine, de la vie privée et de la protection des données à caractère personnel devrait être garanti lors du traitement de données à des fins d'emploi, notamment pour permettre aux employés le développement libre de leur personnalité et afin de préserver la possibilité de relations sociales et individuelles sur leur lieu de travail* ».

En conséquence, la Commission appelle l'attention des employeurs sur le fait que les informations nominatives exploitées dans le cadre des traitements qui sous-tendent les dispositifs d'enregistrement des conversations téléphoniques ne sauraient être détournées de la finalité pour laquelle elles ont initialement été collectées.

En outre, ces dispositifs ne sauraient donner lieu à des pratiques abusives portant atteinte aux libertés et droits fondamentaux des collabora-

teurs, mais également aux droits conférés par la Loi aux Délégués du Personnel et aux Délégués Syndicaux.

Ainsi, l'employeur ne peut pas mettre en place un dispositif d'écoute ou d'enregistrement **permanent ou systématique**, sauf texte légal (par exemple, pour les services d'urgence).

L'employeur ne peut pas non plus enregistrer tous les appels pour lutter contre les incivilités. Il doit choisir un moyen moins intrusif (par exemple opter pour un système permettant au salarié de déclencher l'enregistrement en cas de problème).

Enfin, la Commission préconise que soit instaurée une modalité permettant d'avoir une conversation d'ordre privé non enregistrée, notamment par la mise à disposition d'un « ***téléphone blanc*** » **non enregistré** ou en laissant **la possibilité aux salariés d'utiliser leurs téléphones personnels.**

➢ ***Modalités d'information des personnes concernées***

L'enregistrement des conversations téléphoniques étant un traitement particulièrement intrusif dans la vie professionnelle et privée autant de l'appelant que de l'appelé, la Commission insiste particulièrement sur la nécessaire information des personnes concernées.

A ce titre, l'existence d'un tel traitement d'informations nominatives doit être portée à la connaissance desdites personnes, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Les collaborateurs doivent être informés de la manière la plus efficiente possible. Ainsi, à des fins de transparence, il conviendra d'instaurer une procédure écrite décrivant avec précision, notamment, le déroulement de la procédure de contrôle, ses modalités, les appareils téléphoniques concernés (fixes ou mobiles), la finalité des contrôles envisagés et les modalités de droit d'accès.

Concernant les clients et les tiers la Commission demande que ceux-ci soient informés de l'enregistrement : par le biais d'une clause contractuelle, par l'envoi d'un courrier à titre informatif mentionnant la finalité du traitement et les modalités d'exercice du droit d'accès, **ou par un message vocal.**

➢ ***Données collectées et traitées***

Conformément à l'article 10-1 de la Loi n°1.165 du 23 décembre 1993, la Commission considère que seules les catégories d'informations suivantes peuvent être traitées :

- identité : voix de l'appelant et de l'appelé ;
- contenu de la conversation téléphonique ;
- adresses et coordonnées : numéros de téléphone de l'appelant et de l'appelé ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux enregistrements ;

- données de connexion : logs, traces d'exécution, horodatage, fichiers journaux.

La vidéosurveillance

De nombreuses employeurs ont de plus en plus recours à des systèmes de surveillance afin, par exemple, d'assurer la sécurité des personnes ou des biens ou de contrôler les accès aux locaux.

Ces systèmes utilisent des moyens, plus ou moins complexes, nécessitant le recours à des outils numériques et informatiques, voire à des systèmes de vidéosurveillance.

Ils conduisent souvent à recueillir des informations permettant d'identifier une personne physique déterminée ou déterminable, et soulèvent donc des problèmes particuliers en matière de protection des informations nominatives.

➢ ***Fonctionnalités autorisées***

La Commission considère que, compte tenu du caractère intrusif des dispositifs de vidéosurveillance traitant les informations nominatives et des informations qui peuvent y être associées, la mise en œuvre de tels dispositifs n'est admissible que dans le cadre des impératifs sécuritaires suivants :

- assurer la sécurité des personnes ;
- assurer la sécurité des biens ;
- permettre le contrôle d'accès ;
- permettre la constitution de preuve en cas d'infraction.

A ces impératifs peuvent s'ajouter des fonctionnalités propres à l'activité de l'employeur concerné comme, par exemple, l'évaluation du matériel et des effectifs sur le chantier lorsque ledit employeur est une société de travaux publics.

➢ ***Garanties pour la vie privée des salariés***

Il appartient à l'employeur de démontrer que les droits et libertés des personnes concernées seront protégés.
En conséquence, la Commission demande à l'employeur de préciser que le dispositif de vidéosurveillance mis en œuvre :

- ne permet pas de contrôler le travail ou le temps de travail du personnel ;
- ne conduit pas à un contrôle permanent et inopportun des personnes concernées.

C'est ainsi qu'elle considère que les caméras peuvent filmer :

- les entrées et sorties des bâtiments, en faisant attention toutefois à ne filmer que la surface strictement nécessaire ;
- les issues de secours et les voies de circulation internes ;
- les couloirs ;
- les lieux de stockage de marchandises ;
- les machines de production ;
- les locaux techniques ;
- les archives ;

- les lieux pouvant être considérés comme sensibles (ex : salles serveurs) ;
- le parking intérieur, extérieur et/ou souterrain à condition de ne pas filmer la voie publique ;
- les zones de livraison ou de chargement, les quais de livraison et de déchargement ;
- les caisses.

La Commission estime toutefois que l'installation de dispositif de vidéosurveillance est strictement interdite dans :

- les ateliers (production, montage/démontage...) où travaillent des employés ;
- les vestiaires, les cabinets d'aisance, les bains-douches, les toilettes ;
- les bureaux ainsi que tous lieux privatifs mis à la disposition des salariés à des fins de détente ou de pause déjeuner ;
- les locaux syndicaux et leurs accès lorsque ceux-ci ne mènent qu'à ces seuls locaux.

Par ailleurs, elle rappelle que les caméras ne doivent pas filmer les employés à leur poste de travail, sauf circonstances particulières dûment justifiées. Ainsi, une caméra pourra par exemple filmer un employé manipulant de l'argent mais elle devra être orientée de manière à filmer davantage la caisse que le caissier.

➢ ***Modalités d'information des personnes concernées***

Conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, tout système de vidéosurveillance doit être porté à la connaissance des personnes concernées.

Si l'employeur est libre de choisir le moyen d'information qu'il estime le plus adapté à sa structure ou activité, la Commission demande toutefois que l'information soit dispensée, dans tous les cas, par le biais d'un **panneau d'affichage** mentionnant de manière visible, lisible, claire et permanente l'existence de ce dispositif et comportant, a minima :

- un pictogramme représentant une caméra ;
- le nom du service auprès duquel s'exerce le droit d'accès.

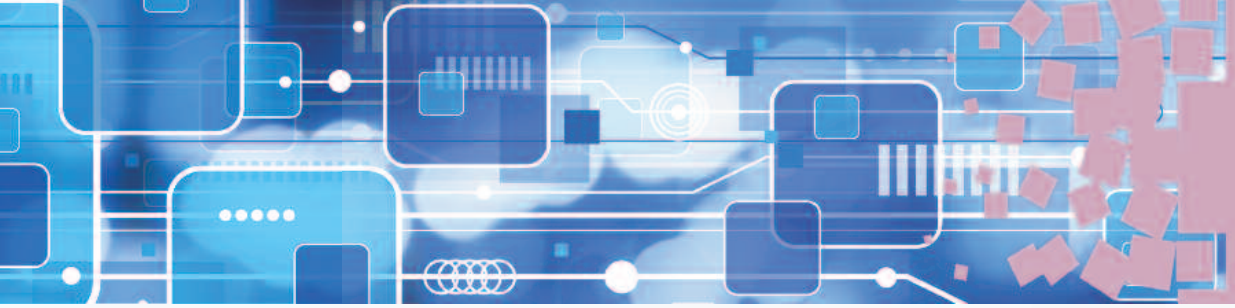
➢ ***Données collectées et traitées***

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

La Commission considère donc que les informations suivantes peuvent être collectées et traitées :

- identité : image, visage et silhouette des personnes ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux images ;
- informations temporelles et horodatage : lieu et identification de la caméra, date et heure de la prise de vue.

Concernant la collecte de la voix dans le cas de l'exploitation d'un système de vidéosurveillance, la Commission considère le plus souvent qu'une telle collecte est manifestement excessive au regard des fonctionnalités du traitement. En effet, la collecte de la voix en vue, par exemple, d'assurer la sécurité des biens et des personnes peut conduire à une



surveillance pouvant être inopportune à l'égard des personnes concernées. La Commission est donc particulièrement attentive à la justification apportée par l'employeur.

➢ ***Durée de conservation des données***

Conformément à l'article 10-1 de la Loi n°1.165 du 23 décembre 1993, les données ne doivent être conservées que « *pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées* », à savoir **un mois**.

La géolocalisation

Les dispositifs dits de géolocalisation des véhicules permettent aux employeurs de connaître la position géographique, à un instant donné ou en continu, des employés par la localisation des véhicules qui leur sont confiés. Or, si ces systèmes sont susceptibles d'améliorer les services rendus par les entreprises, leur usage peut donner lieu à des dérives qu'il convient de prévenir.

➢ ***Fonctionnalités autorisées***

La Commission considère que, compte tenu du caractère intrusif des dispositifs traitant la donnée de géolocalisation des véhicules et des informations qui peuvent y être associées, la mise en œuvre de tels dispositifs n'est admissible que dans le cadre des fonctionnalités suivantes :

- la sûreté ou la sécurité de l'employé lui-même ou des marchandises ou véhicules dont il a la charge (chauffeurs de véhicules de remise, travailleurs isolés, transports de fonds et de valeurs, etc.) ;
- une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés, (interventions d'urgence, flottes de dépannage, etc.) ;
- le suivi et la facturation d'une prestation de transport de personnes ou de marchandises ou d'une prestation de services directement liée à l'utilisation du véhicule (ramassage scolaire, nettoyage des accotements, etc.) ;
- le suivi du temps de travail, lorsque ce suivi ne peut être réalisé par d'autres moyens.

➢ ***Garanties pour la vie privée des salariés***

Pour la Commission, l'utilisation d'un dispositif de géolocalisation ne doit pas conduire à un contrôle permanent et inopportun de l'employé concerné. Aussi :

- s'agissant des véhicules professionnels pouvant être utilisés par les employés à des fins privées, l'employeur ne doit pas collecter des informations relatives à la localisation d'un employé en dehors des horaires de travail de ce dernier. Dans ce contexte, elle exige que ces derniers aient la possibilité de désactiver la fonction de géolocalisation des véhicules à l'issue de leur temps de travail ;
- concernant les employés investis d'un mandat électif ou syndical, ceux-ci ne doivent pas faire l'objet d'une opération de géolocalisation lorsqu'ils agissent dans le cadre de l'exercice de leur mandat ;
- l'utilisation d'un système de géolocalisation n'est pas justifiée lorsqu'un employé dispose d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP, etc.).

➢ ***Modalités d'information des salariés***

Nonobstant l'information collective prévue par des conventions collectives professionnelles, la Commission demande que l'employé soit clairement et individuellement informé, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 :

- de l'identité du responsable de traitement ;
- de la finalité du traitement ;

- du caractère obligatoire ou facultatif du dispositif ;
- e l'identité des destinataires ou des catégories de destinataires des informations ;
- de l'existence de ses droits d'accès, de rectification et le cas échéant de son droit d'opposition relativement aux informations le concernant.

Les contrôles d'accès par badges

Ces dispositifs utilisent des moyens plus ou moins complexes, nécessitant le recours à des outils numériques et/ou informatiques, voire à des systèmes de communications électroniques.

Il peut s'agir de cartes magnétiques ou cartes à puce, avec ou sans contact, combinées à un dispositif de lecture desdites cartes, qui enregistre ou non les informations qu'elles contiennent. D'autres types de dispositifs sont également utilisés, tels que des codes secrets délivrés aux seules personnes habilitées ou des systèmes d'ouverture de portes à distance par le biais d'un poste téléphonique géré par autocommutateur.

Ainsi, l'essence même de tels systèmes repose dans la nécessaire identification des personnes aux fins de surveiller ceux qui pénètrent sur le lieu de travail ou dans certaines zones à accès restreint.

Cette surveillance s'étend donc aussi bien à leur identité, qu'à la date, l'heure et la porte par laquelle ils ont pu accéder aux locaux.

➢ ***Fonctionnalités autorisées***

La Commission considère que la mise en œuvre de dispositifs de contrôle d'accès ne peut avoir d'autres fonctionnalités que :

- de contrôler l'accès aux entrées et sorties de l'entreprise ;
- de contrôler l'accès à certains locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent ;
- de gérer les horaires et les temps de présence des employés ;
- de contrôler l'accès des visiteurs ;
- de permettre, le cas échéant, la constitution de preuves en cas d'infraction.

➢ ***Garanties pour la vie privée des salariés***

Ces dispositifs ne sauraient être détournés de leur finalité. Ainsi, ils ne peuvent en aucun cas :

- onduire à un contrôle permanent et inopportun des personnes concernées ;
- permettre le contrôle des quotas d'heures que la Loi confère aux Délégués du Personnel et aux Délégués Syndicaux pour l'exercice de leurs fonctions ;
- permettre le contrôle des déplacements à l'intérieur de l'entreprise, exception faite des zones limitativement identifiées comme faisant l'objet d'une restriction de circulation.

➢ ***Modalités d'information des personnes concernées***

L'existence de tout traitement relatif à un contrôle d'accès par badges doit être portée à la connaissance des personnes concernées, à savoir les

employés et visiteurs, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Aux termes de cet article, cette information doit porter sur :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'identité des destinataires ou des catégories de destinataires des informations ;
- l'existence d'un droit d'opposition, d'accès et de rectification à l'égard des informations les concernant.

Les modalités de communication de cette information sont laissées au libre choix de l'employeur. Pour les employés, cette communication peut par exemple s'effectuer par voie d'affichage ou par la communication d'une note interne à l'entreprise.

Concernant les visiteurs, cette information pourrait par exemple prendre la forme d'une mention portée sur le formulaire de collecte des informations personnelles qu'ils remplissent, le cas échéant.

Les contrôles d'accès par des dispositifs biométriques

Dans un contexte où se mêlent technologie et sécurité, la biométrie tend à s'imposer dans un certain nombre de pays comme une méthode privilégiée d'identification dans les entreprises.

Pour la Commission toutefois, la donnée biométrique n'est pas une donnée d'identité comme les autres. En effet, elle n'est pas attribuée par un tiers ou choisie par la personne. Elle provient de son corps lui-même et le désigne de façon définitive. Le mauvais usage ou le détournement d'une telle donnée peut alors avoir des conséquences graves. C'est pour cela que le recours à la biométrie doit être strictement encadré.

➢ **Traitement reposant sur la reconnaissance du contour de la main**

• **Fonctionnalités autorisées :**

La Commission considère que la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main ne peut avoir d'autres fonctionnalités que de :

- contrôler l'accès aux entrées et sorties de l'entreprise ;
- contrôler l'accès à certains locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent ;
- gérer les horaires et les temps de présence des employés ;
- contrôler l'accès des visiteurs ;
- permettre, le cas échéant, la constitution de preuve en cas d'infraction.

• **Données collectées et traitées :**

Conformément aux principes d'adéquation et de proportionnalité des informations nominatives collectées, posés par l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, la Commission estime que seules les catégories d'informations suivantes peuvent être traitées :

- Donnée biométrique : gabarit du contour de la main (résultat du traitement des mesures du contour de la main par un algorithme) ;
- Informations relatives à l'identité de l'employé : nom, prénoms, code d'authentification, photographie ;
- Informations relatives à la vie professionnelle : numéro d'identification interne, service, fonction ;
- Informations sur le temps de présence ou horodatage : date et heure d'entrée et de sortie, plages horaires autorisées, date et heure de passage à une zone à accès restreint, cumul des horaires, heures supplémentaires, absences, autorisations d'absence, congés ;
- Accès aux locaux : nom et/ou numéro de la porte d'entrée ou de sortie, ou du point de passage, zones d'accès autorisé ;
- Parking : numéro d'immatriculation du véhicule, numéro de la place de stationnement ;
- Visiteurs : informations d'identité, dates et heures de passage, porte utilisée, organisme ou société d'appartenance, identité de l'employé accueillant le visiteur, gabarit du contour de la main.

• Durée de conservation :

- la donnée biométrique et le code d'authentification associé doivent être supprimés dès le départ de l'employé de l'entreprise ;
- les informations relatives à l'identité de l'employé, à la vie professionnelle et à la gestion du parking ne doivent pas être conservées au-delà d'une durée de 5 ans après son départ de l'entreprise ;
- les données relatives à l'accès aux locaux et aux informations sur le temps de présence ou d'horodatage ne doivent pas être conservées plus de 3 mois. Elles pourront être conservées 5 ans dans la seule hypothèse où l'employeur exploite ce dernier à des fins de contrôle du temps de travail et pour les employés uniquement ;
- s'agissant des visiteurs, les informations relatives à la donnée biométrique, à l'identité, à la vie professionnelle, et à la gestion du parking ne doivent pas être conservées au-delà d'une durée de 3 mois à compter de la dernière visite.

➢ Traitement reposant sur la reconnaissance du réseau veineux des doigts de la main

• Fonctionnalités autorisées :

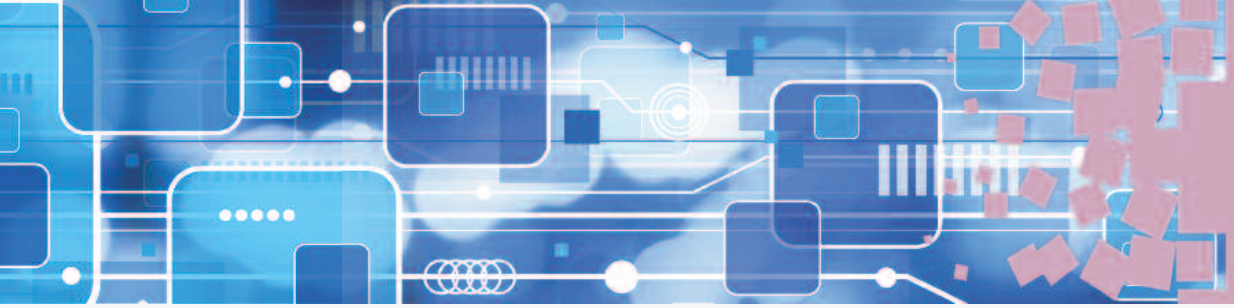
La Commission considère que la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main ne peut avoir d'autres fonctionnalités que de :

- contrôler l'accès aux entrées et sorties de l'entreprise ;
- contrôler l'accès à certains locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent ;
- contrôler l'accès des visiteurs ;
- permettre, le cas échéant, la constitution de preuves en cas d'infraction.

• Données collectées et traitées :

Conformément aux principes d'adéquation et de proportionnalité des informations nominatives collectées, posés par l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, la Commission estime que seules les catégories d'informations suivantes peuvent être traitées :

- Donnée biométrique : Gabarit du réseau veineux du doigt de la personne ;



- Informations relatives à l'identité de l'employé : nom, prénoms, photographie ;
- Informations relatives à la vie professionnelle : numéro d'identification interne, service, fonction ;
- Informations temporelles ou horodatage : date et heure d'entrée et de sortie, date et heure de passage à une zone à accès restreint, plages horaires d'accès autorisées ;
- Accès aux locaux : nom et/ou numéro de la porte d'entrée ou de sortie, ou du point de passage, zone d'accès autorisées ;
- Parking : numéro d'immatriculation du véhicule, numéro de la place de stationnement ;
- Visiteurs : informations d'identité, dates et heures de passage, porte utilisée, organisme ou société d'appartenance, identité de l'employé accueillant le visiteur, gabarit du réseau veineux du doigt.

• Durée de conservation :

- les informations relatives à l'identité d'un employé, à la vie professionnelle et au parking ne doivent pas être conservées au-delà d'une durée de 5 ans après le départ de l'employé de l'entreprise ou de l'organisme, et les informations relatives aux informations temporelles ou horodatage ne doivent pas être conservées plus de 3 mois à compter de leur collecte ;
- les informations relatives aux visiteurs ainsi que les informations temporelles ou d'horodatage, et celles concernant les accès, ne doivent pas être conservées au-delà d'une durée de 3 mois à compter de la dernière visite ;
- le gabarit de l'empreinte biométrique doit être supprimé dès le départ de l'employé.

➢ ***Traitement reposant sur la reconnaissance de l'empreinte digitale***

• Fonctionnalités autorisées :

La Commission considère que la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale, enregistrée sur un support individuel détenu par la personne concernée, **ne peut avoir d'autre fonctionnalité que de contrôler l'accès à certaines zones limitativement identifiées au sein de l'entreprise comme faisant l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent.**

Elle interdit par ailleurs les dispositifs :

- enregistrant une image ou une photographie de l'empreinte digitale ;
- reposant sur la reconnaissance de l'empreinte digitale **avec stockage dans une base de données centralisée ou sur un terminal de lecture-comparaison.**

• Garanties pour la vie privée des salariés :

Le dispositif reposant sur la reconnaissance de l'empreinte digitale présentant plus de risques pour les individus que celui relatif au contour de la main ou au réseau veineux des doigts de la main, la Commission **exclut l'utilisation de cette donnée à des fins de gestion des horaires et des temps de présence des employés, ou à des fins de contrôle d'accès aux entrées et sorties de l'entreprise.**

Par ailleurs, ces dispositifs ne sauraient être détournés de leur finalité, et notamment ils ne peuvent en aucun cas conduire à un contrôle permanent et inopportun des employés.

Enfin, la Commission estime que les contrôles d'accès aux zones concernées ne doivent pas entraver la liberté d'aller et de venir des salariés protégés dans l'exercice de leurs missions.

• **Données collectées et traitées :**

Conformément aux principes d'adéquation et de proportionnalité des informations nominatives collectées, posés par l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, la Commission estime que seules les catégories d'informations suivantes peuvent être traitées :

- Donnée biométrique : gabarit de l'empreinte digitale ;
- Informations relatives à l'identité de l'employé : nom, prénoms, photographie ;
- Informations relatives à la vie professionnelle : numéro d'identification interne, numéro de carte, service, fonction ;
- Informations temporelles ou horodatage : date et heure de passage à une zone à accès restreint, plages horaires d'accès autorisées ;
- Accès aux locaux à accès restreint : nom et/ou numéro du point de passage à la zone à accès restreint, zones d'accès autorisées ;
- Tiers autorisé : nom, prénoms, dates et heures de passage à la zone à accès restreint, organisme ou société d'appartenance, identité de l'employé accueillant le tiers autorisé.

• **Durée de conservation :**

- les informations relatives à l'identité d'un employé et à sa vie professionnelle ne doivent pas être conservées au-delà d'une durée de 5 ans après le départ de l'employé de l'entreprise ;
- les informations relatives aux tiers autorisés, ainsi que les informations temporelles ou d'horodatage, et celles concernant les accès, ne doivent pas être conservées au-delà d'une durée de 3 mois à compter du dernier passage ;

- le gabarit de l'empreinte biométrique n'est conservé sur le support individuel que le temps durant lequel la personne concernée est habilitée à pénétrer dans les locaux ou les zones limitativement identifiées de l'entreprise faisant l'objet d'une restriction de circulation.

➢ ***Modalités d'information des personnes concernées par tout traitement de contrôle d'accès reposant sur des dispositifs biométriques***

L'existence de tout traitement relatif à un contrôle d'accès par un dispositif biométrique doit être portée à la connaissance des personnes concernées, à savoir les employés et visiteurs, conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Aux termes de cet article, cette information doit porter sur :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'identité des destinataires ou des catégories de destinataires des informations ;
- l'existence d'un droit d'opposition, d'accès et de rectification à l'égard des informations les concernant.

Les modalités de communication de cette information sont laissées au libre choix de l'employeur. Pour les employés, cette communication peut par exemple s'effectuer par voie d'affichage ou par la communication d'une note interne à l'entreprise.

Concernant les visiteurs, cette information pourrait par exemple prendre la forme d'une mention portée sur le formulaire de collecte des informations personnelles qu'ils remplissent, le cas échéant.

Limitation des personnes ayant accès aux informations

Quels que soient les dispositifs mis en place, la Commission considère que l'accès aux informations objets du traitement doit être limité aux seules personnes qui, dans le cadre de leurs attributions, peuvent légitimement en avoir connaissance au regard de la finalité du traitement ou du but recherché.

C'est ainsi, par exemple, qu'elle estime que dans le cadre d'un dispositif de contrôle d'accès par badges non biométriques, les catégories de personnel suivantes pourront avoir accès à certaines des informations collectées :

✓ service du personnel / ressources humaines : identité des employés, informations relatives à la vie professionnelle, informations temporelles et horodatage, numéro d'identification interne ;

✓ service comptable / de paie : identité des employés, informations relatives à la vie professionnelle, informations temporelles et horodatage, numéro d'identification interne ;

✓ service gérant la sécurité des locaux : identité des employés, informations relatives aux visiteurs, accès aux locaux, parking, informations temporelles.

LE WIFI, QUELLES PRATIQUES POUR LES RESPONSABLES DE TRAITEMENTS ET LES UTILISATEURS ?

Nous avons tous l'habitude d'utiliser le WIFI pour nous connecter à Internet, à la maison, au travail, dans les lieux publics. Toutefois, pour l'utilisateur, ce geste habituel ne revêt pas la même sensibilité en fonction du lieu dans lequel s'opère la connexion.

En outre pour les entreprises mettant à disposition un accès WIFI, certaines obligations légales pèsent sur elles, différentes en fonction de la finalité pour laquelle l'accès est ouvert. Cette fiche pratique s'attache à résumer les réflexes à adopter pour toutes les catégories de personnes concernées par de tels traitements.

Le WIFI, Kézaco ?

Wi-Fi est une marque détenue par le consortium Wi-Fi Alliance.

Un constructeur informatique ou un fabricant de smartphones fournissant un produit compatible avec une des normes IEEE 802.11 (réseau sans fil) doit demander à la Wi-Fi Alliance (anciennement WECA) le droit d'apposer le nom Wi-Fi et le logo correspondant.

Le terme « Wi-Fi » est aujourd'hui largement connu pour être la contraction de « *Wireless Fidelity* » cependant cette explication est quelque peu erronée...

En effet le consortium Wi-Fi Alliance avait demandé à une agence de publicité de lui proposer un nom plus facile à utiliser que « IEEE 802.11b Direct Sequence Spread Spectrum ».

L'agence lui a proposé plusieurs noms ; parmi ceux-ci, la « Wi-Fi Alliance qui sonnait un peu comme « Hi-Fi », une marque reconnue dans un autre domaine.....

Le Wi-Fi repose sur la norme IEEE 802.11. Il s 'agit d'une technologie dite « *sans fil* » qui permet la connexion de tout type de matériel (ordinateurs portables, tablettes, imprimantes, téléphones mobiles, consoles de jeux, télévisions, équipements électroménagers, automates industriels, etc.) à des réseaux professionnels privés ainsi qu'au réseau public, Internet.

De la même façon que le fait votre téléphone mobile, la technologie « *Wi-Fi* » utilise des ondes radio pour transmettre des données à travers un réseau, tout équipement utilisant le wifi possède donc un adaptateur réseau sans fil qui traduira les données envoyées en un signal radio.

Ce même signal est alors transmis, par l'intermédiaire d'une antenne (Hotspot), à un décodeur : le routeur. Les données, une fois décodées, seront envoyées à l'Internet via une connexion filaire ou optique de la « box » vers l'opérateur.

Le terme « *Hotspot* » est utilisé pour définir une zone où la connexion Wi-Fi est disponible.

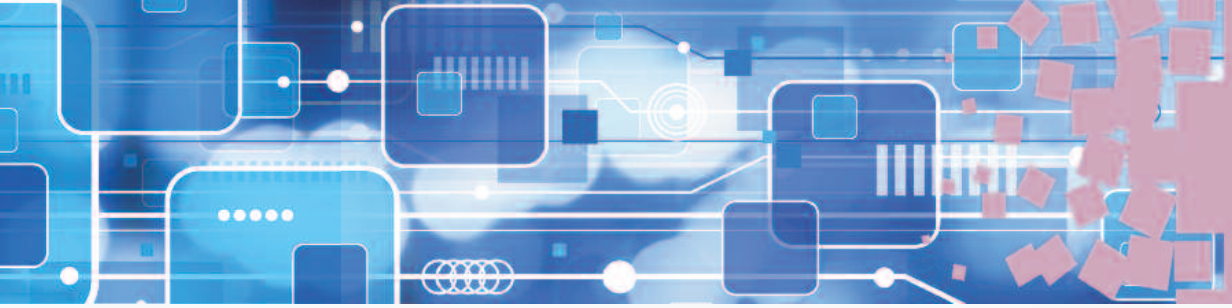
Vous êtes utilisateur de WIFI, quels risques et quelles précautions prendre hors de chez vous ?

Selon une étude publiée en juillet 2017 par la société de sécurité informatique Norton by Symantec, 87% des Français mettent en danger leurs informations personnelles en se connectant à un Wi-Fi public. De nombreux consommateurs sont convaincus que l'usage d'un mot de passe pour l'accès au Wi-Fi garantit la sécurité de leurs informations : ce n'est pas le cas.

Comme son nom l'indique, un Wifi-public est « *ouvert* », il n'y a pas vraiment besoin de code pour se connecter. Parfois, une adresse e-mail est demandée pour y accéder.

La principale caractéristique qui intéresse les personnes mal intentionnées est que les Wifi-publics ne sont pas chiffrés, mais d'autres risques existent, même en l'absence de mauvaise intention de la personne mettant à disposition le Wifi, tels que :

- Une collecte trop importante d'informations vous concernant ; par exemple, la CNIL a constaté qu'il est fréquent que des données portant sur le contenu des correspondances échangées ou des informations consultées (URLs) sont conservées alors que les fournisseurs du service ne sont pas autorisés à le faire ;
- Une conservation trop importante d'informations vous concernant : la CNIL a relevé que la plupart des fournisseurs de service conservent les données issues des journaux de connexion sans qu'aucune durée de conservation n'ait été définie. Or, les données de trafic doivent être conservées pendant 1 an à compter du jour de leur enregistrement ;
- Une surveillance directe du trafic internet visité.



Dès lors :

- Lors d'une connexion à un Wi-Fi gratuit, assurez-vous au préalable de n'être connecté à aucune de vos applications ;
- Ne visitez pas de pages (site web) requérant un login et mot de passe. Visitez uniquement des pages authentifiées (HTTPS). Bien réfléchir avant de cliquer sur un lien ;
- Couper « l'application » Wi-Fi si elle n'est pas utilisée, et notamment la reconnexion automatique : dans le cas contraire, si vous vous connectez à un point d'accès malveillant, votre équipement pourrait bien s'en souvenir et s'y reconnecter automatiquement lorsque ce point d'accès sera de nouveau à portée de connexion ;
- Garder en permanence le terminal à jour ;
- Certains réseaux Wi-Fi sont complètement fictifs et n'existent que pour récupérer des données. Restez donc vigilant. N'hésitez pas à vérifier la légitimité d'un réseau.

D'une manière générale :

- Evitez de passer par un Wi-Fi public pour transmettre/recevoir des données personnelles, surtout si celui-ci vous est inconnu ;
- Evitez de confier trop de données personnelles en échange d'un accès Wifi gratuit ;
- Préférez passer par le réseau 3G/4G/5G de votre opérateur internet. Si vous n'avez pas le choix, privilégiez toujours la visite de sites HTTPS ;
- Optez pour un abonnement VPN qui apporte un chiffrement de bout en bout assurant la confidentialité des données que vous envoyez et recevez.

Vous êtes responsable de traitement et vous mettez à disposition du public un accès Internet par WIFI :

- **Vous êtes concernés par les dispositions de l'article 10 de la Loi n° 1.430 sur la préservation de la sécurité nationale, et de son Arrêté Ministériel d'application**

En effet, l'article 1er 2° de l'Arrêté Ministériel portant application l'article 10 de la Loi précitée dispose que sont notamment qualifiés d' « *opérateurs et prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques (...) les personnes qui offrent un accès à des services de communications électroniques au public en ligne, y compris à titre gratuit (...)* », donc les responsables de traitement proposant du WIFI à titre gracieux, ou non, pour leurs clients ou visiteurs.

A cet égard, ils doivent donc collecter, « à l'exclusion des contenus des correspondances échangées (...)- Pour les personnes visées au chiffre 2° de l'article premier :

1° l'identifiant de la connexion ;

2° l'identifiant attribué par ces personnes à l'abonné ;

3° l'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;

4° les dates et heure de début et de fin de la connexion ;

5° les caractéristiques de la ligne de l'abonné.

- Pour les personnes visées au chiffre 3 et au chiffre 2, lorsque ces dernières les collectent pour leurs propres besoins :

1° l'identifiant de la connexion au moment de la création du compte ;

2° les nom et prénom ou la raison sociale ;

3° les adresses postales associées ;

4° les pseudonymes utilisés ;

5° les adresses de courrier électronique ou de compte associés ;

6° les numéros de téléphone ;

7° le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ;

8° le type de paiement utilisé ;

9° la référence du paiement ;

10° le montant ;

11° la date et l'heure de la transaction.

Peuvent également être recueillies, auprès de l'ensemble des personnes visées à l'article premier, les données techniques relatives :

1° à la localisation des équipements terminaux ;

2° à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;

3° à l'acheminement des communications électroniques par les réseaux ;

4° à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ;

5° aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels ».

- **Dès lors, eu égard à la collecte d'informations nominatives, vous devez effectuer une formalité auprès de la CCIN**

Il s'agit d'une déclaration ordinaire, qui aura pour principales caractéristiques :

- mise à disposition d'un accès Internet par le biais d'une borne WIFI ;
- informer les personnes concernées par le biais d'une fenêtre ou par l'acceptation de conditions générales ;
- collecter les éléments d'identification et les logs de connexion d'une personne concernée pour une durée d'un an ;
- restreindre l'accès à des sites indésirables.

Et vous devez faire attention aux risques de sécurité pour votre système d'information si votre réseau WIFI n'est pas étanche (sécurisé)

En tout état de cause, collectez des données proportionnées à la finalité de la mise à disposition du WIFI.

ATTENTION : les dispositions de la Loi n° 1.430 ne semblent pas s'appliquer si vous êtes un employeur cloisonnant le wifi à une utilisation par ses salariés. Dans ce cas, il ne s'agit que d'une modalité particulière de connexion par l'entreprise au réseau Internet, qui est couverte par la formalité de déclaration simplifiée de « *Gestion administrative des salariés* ». Toutefois, tout outil de surveillance de consommation de l'Internet doit être soumis à autorisation de la CCIN et les personnes concernées (les salariés) doivent être informées de cette surveillance et de leurs droits, ceci que la connexion au réseau soit filaire ou par WIFI.

Commission de Contrôle des Informations Nominatives - 10ème Rapport d'Activité Annuel 2018

www.stilelibero.mc - Images : Istockphoto, Fotolia, Shutterstock, Freepik, SLC, Pexel, Pixbay.

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