CCIN

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

RAPPORT D'ACTIVITÉ 2020

12ème rapport public

LE MESSAGE DU PRÉSIDENT

L'activité de la CCIN a été tout particulièrement soutenue en 2020. En effet la Commission a dû, comme tout un chacun, faire preuve de réactivité, mais aussi de vigilance, dans un contexte totalement inédit mettant en balance la préservation de la santé publique et la protection des droits et des libertés individuelles.

Si notre Commission ne peut qu'être totalement solidaire, et compréhensive des impératifs résultant de la crise sanitaire, elle a néanmoins constaté une imprégnation insuffisante à la protection des données de santé dans des situations nécessitant la mise en œuvre de mesures en urgence pour tenter d'endiguer la propagation du virus.

Ainsi les effets de cette pandémie, qui se font encore ressentir aujourd'hui, ont donné lieu à des saisines extrêmement tardives de la CCIN par les Autorités Gouvernementales, alors que les décisions avaient déjà été prises en amont, sans réelle volonté de les réorienter. Nous avons également déploré une absence de consultation sur des sujets pourtant majeurs au regard de leurs impacts sur le respect dû à la vie privée de chacun. Ceci a également été constaté dans des domaines sans lien avec la crise sanitaire.

Pourtant les dispositions légales qui nous régissent prévoient que notre Commission soit obligatoirement consultée lors de l'élaboration de mesures législatives ou réglementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement des informations nominatives.

Je voudrais ici souligner que la protection des données personnelles n'est en rien un obstacle à la gestion d'une telle crise sanitaire. Elle doit à l'inverse faire partie intégrante du processus décisionnel et assurer ainsi une juste proportion entre les atteintes aux libertés individuelles résultant d'un tel contexte et le nécessaire respect des droits fondamentaux.

Il importe que chacun en prenne conscience.

L'année 2020 a également été marquée par la consultation de notre Commission sur le projet de loi relative à la protection des données personnelles, dont l'objectif est d'introduire en droit interne les standards internationaux résultant tout à la fois de la Convention 108 + du Conseil de l'Europe, du Règlement Général européen sur la Protection des Données et de la Directive « Police Justice ».

Nous n'avons pu que nous féliciter d'avoir été associés dès l'origine à l'élaboration de ce projet de texte, donnant ainsi l'occasion à la CCIN de porter en amont une attention particulière aux éléments essentiels de nature à permettre que la Principauté puisse enfin bénéficier d'une décision d'adéquation de la part de la Commission européenne.

Toutefois, nous avons constaté que de nombreuses modifications ont été introduites au fil des mois. La version sur laquelle la CCIN a été officiellement saisie est le fruit d'arbitrages gouvernementaux sur des sujets revêtant une acuité certaine en matière de préservation de la vie privée. Tel est notamment le cas s'agissant du champ de compétence de la future Autorité de Protection des Données Personnelles appelée à remplacer la CCIN.

Aussi si ces choix devaient être maintenus dans la nouvelle loi relative à la protection des données personnelles, des dispositions législatives devront, de manière concomitante, apporter aux personnes concernées des garanties suffisantes et effectives dans des domaines potentiellement intrusifs pour le respect de leurs droits, et ce afin de se conformer aux standards internationaux à l'aune desquels sera apprécié le caractère adéquat du droit interne régissant la matière.

Les travaux relatifs à la refonte de la législation relative à la protection des données personnelles ont débuté depuis plusieurs années, et je souhaite me faire l'écho des entités de la Principauté qui appellent de leurs vœux que cette modification intervienne désormais, à brève échéance, cette étape constituant le préalable indispensable au processus d'adéquation de la Principauté dont la reconnaissance revêt une importance toute particulière à l'heure où Monaco entend développer ses offres en matière numérique.

Guy MAGNAN

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

RAPPORT D'ACTIVITÉ 2020

12ème rapport public

Sommaire

LA COMPOSITION DE LA COMMISSION

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

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

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

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

Guy MAGNAN - Président

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

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

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

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

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

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

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

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

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

Rainier BOISSON - Vice Président

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

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

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

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

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

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

Il assume depuis le mois d'octobre 2018 la Présidence du Conseil du Patrimoine.

Florestan BELLINZONA - Commissaire

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

Après une expérience de six mois au Bureau Permanent de la Conférence de La Haye de droit international privé, il est nommé Juge suppléant en octobre 2003 puis Juge en 2005 avant d'accéder aux fonctions de Premier Juge en 2013, et de Vice-Président du Tribunal de Première Instance depuis octobre 2020.

Ayant été successivement Juge des accidents du travail, Juge tutélaire en charge des affaires familiales puis Juge de l'application des peines, il est actuellement Président de la formation correctionnelle statuant sur intérêts civils et Président de la formation correctionnelle pour mineurs. Il préside également les audiences de flagrant délit.

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

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

Philippe BLANCHI - Commissaire

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

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

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

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

Robert CHANAS - Commissaire

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

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

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

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

La même année, il devient Agent Comptable.

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

Jean-François CULLIEYRIER - Commissaire

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

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

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

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

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

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

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

Hommage à Monsieur Jean Yves PEGLION, Commissaire

décédé le 9 janvier 2021

Titulaire d'un Diplôme d'Etudes Commerciales Supérieures Jean-Yves Peglion avait débuté 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 était retourné à l'Office Monégasque des Téléphones au sein de la Direction Administrative et Financière puis il avait accédé aux fonctions de Vérificateur Principal des Finances au Contrôle Général des Dépenses avant d'intégrer la Mairie en 2008, dont il a été le Secrétaire Général jusqu'en avril 2013, date à laquelle il avait pris sa retraite.

Durant ces cinq années au sein de l'Administration Communale il avait travaillé notamment sur le déploiement de la carte d'identité monégasque électronique, la réorganisation et le transfert de Services Communaux au Foyer Sainte Dévote, ainsi que l'organisation de deux élections, communales en 2011 et nationales en 2013.

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

Président de Monaco Mutualité, ses compétences en matière de fonctionnement des organismes de prestations médicales ont également permis à la Commission une meilleure compréhension des spécificités de ce domaine qui requiert une sensibilité forte à la préservation de la vie privée.

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

La Commission et son Secrétariat Général tiennent à rendre hommage à Monsieur Jean Yves PEGLION qui fut Commissaire pendant plus de 6 ans.

Au cours de ces années, il a su, avec bon sens, pragmatisme et détermination, alimenter les débats de la Commission et les enrichir de ses connaissances pointues du fonctionnement de l'Administration.

Il laisse à chacun le souvenir d'un homme de conviction, rigoureux et compréhensif.

01

LES MISSIONS ET LE FONCTIONNEMENT DE LA COMMISSION

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

Afin que la protection des informations nominatives, garantie par le droit interne monégasque, soit en adéquation avec les standards européens tels qu'ils sont encadrés par la Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel relatif aux Autorités de contrôle et aux flux transfrontières de zdonnées, 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 Judiciaires 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 renouvelables sans restriction, à cinq ans renouvelables une fois. De plus le Président est désormais élu par ses pairs et non plus nommé par Ordonnance Souveraine.

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

UNE MISSION D'INFORMATION

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

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

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

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

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

UNE MISSION DE PROPOSITION ET DE CONSULTATION

La Commission a également des missions de proposition et de consultation. A cet effet elle est consultée, conformément à l'article 2-14° de la Loi n° 1.165, par le Ministre d'Etat lors de l'élaboration de textes susceptibles d'avoir une incidence sur la protection des droits et libertés des personnes à l'égard du traitement des informations nominatives et peut l'être pour toute autre mesure susceptible d'affecter lesdits droits et libertés.

La CCIN peut également :

- formuler toute recommandation entrant dans le cadre des missions qui lui sont conférées par la Loi, afin d'orienter les responsables de traitements en portant à leur connaissance des principes auxquels devraient répondre leurs traitements automatisés ;
- proposer aux Autorités compétentes des dispositions afin de fixer, soit des mesures générales propres à assurer le contrôle et la sécurité du traitement, soit des mesures spéciales ou circonstancielles, y compris, à titre exceptionnel, la destruction des supports d'informations ;
- proposer ou donner un avis sur l'édiction de normes fixant les caractéristiques auxquelles doivent répondre les traitements ne comportant manifestement pas d'atteinte aux libertés et droits fondamentaux. Ces traitements peuvent faire l'objet d'une déclaration simplifiée de conformité, ou être exonérés de toute obligation de déclaration, dans les conditions prévues par Arrêté Ministériel.

UNE MISSION DE CONTRÔLE *A PRIORI*

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

L'analyse porte sur la vérification des éléments limitativement énumérés à l'article 8 de la Loi n° 1.165. Dans le cadre de la seconde phase de contrôle *a priori*, la Commission analysera l'ensemble du traitement soumis à demande d'avis ou d'autorisation et appréciera si les principes relatifs à la qualité des informations, aux conditions de licéité des traitements et au respect des droits des personnes sont garantis ; elle vérifiera également si les exigences de sécurité et de confidentialité des traitements sont remplies.

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

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

- à l'article 11-1 pour la mise en œuvre par les personnes physiques ou morales de droit privé :
  - de traitements portant sur des soupçons d'activités illicites, des infractions et des mesures de sûreté ;
  - de traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes ;
  - de traitements exploités à des fins de surveillance ;
- à l'article 20-1 pour les transferts d'informations nominatives vers des Pays ou organismes n'assurant pas un niveau de protection adéquat.

UNE MISSION DE CONTRÔLE *A POSTERIORI* : LES INVESTIGATIONS

Deux procédures distinctes

L'investigation à l'initiative de la Commission

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

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

Toutefois, en cas d'urgence ou de risque imminent de destruction ou de disparition de pièces ou de documents, les investigateurs pourront accéder aux locaux sans autorisation préalable du Juge, lequel pourra cependant être saisi par les personnes auxquelles les opérations de contrôle

feraient grief aux fins de déclarer la nullité desdites opérations, par exemple en cas d'invocation manifestement injustifiée de l'urgence.

L'investigation suite à une plainte

Pour sa part l'article 18-2 de la Loi n° 1.165 prévoit une procédure spécifique lorsqu'il existe une raison de soupçonner que la mise en œuvre des

traitements n'est pas conforme à la Loi sur la protection des informations nominatives, sans que le droit d'opposition puisse être invoqué, mais uniquement sur autorisation préalable du Président du Tribunal de Première Instance. L'Ordonnance permettant aux investigateurs d'accéder aux locaux peut faire l'objet d'un recours non suspensif. S'il est fait droit à ce recours, le juge peut alors déclarer la nullité des opérations d'investigation.

Un socle commun

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

Une plage horaire élargie

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

L'opposabilité du secret professionnel

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

Les missions lors du contrôle

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

Cependant les nouvelles dispositions viennent préciser que seul un médecin désigné par le Président de la Commission parmi les médecins figurant sur une liste établie par le Conseil de l'Ordre des médecins et comportant au moins cinq noms, peut requérir la communication d'informations médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins, ou de la gestion de services de santé, et qui est mis en œuvre par un membre d'une profession de santé.

Les contrôles en ligne

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

La consécration du contradictoire

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

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

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

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

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

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

La Commission est de plus habilitée à ester en justice.

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

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

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

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

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

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

Des sanctions administratives

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

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

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

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

LE BUDGET DE LA COMMISSION

Pour l'année 2020 la Commission avait bénéficié au titre du budget primitif d'un montant initial total de 1.457.300,00 € se répartissant ainsi :

907.300,00 €
au titre des crédits de fonctionnement ;

550.000,00 €
au titre de ses dépenses salariales.

Toutefois, afin de contribuer à l'effort budgétaire visant à endiguer le déficit prévisionnel du budget de l'Etat du fait de la crise sanitaire, la CCIN a réduit son budget de fonctionnement de 107.000,00 euros, soit près de 12 %.

Ainsi les frais de fonctionnement de la Commission se sont élevés à 800.300,00 euros.

Cette diminution signification a été rendue possible par l'annulation de l'intégralité des déplacements, le redéploiement des dépenses informatiques et la réduction des frais divers.

L'aménagement des modalités de travail à distance n'a entraîné aucune dépense supplémentaire, l'ensemble des équipements et des dispositifs y afférents ayant déjà été acquis et paramétrés plusieurs mois auparavant.

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.

02

L'ORGANISATION ET LES MISSIONS DU SECRÉTARIAT GÉNÉRAL

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

Outre le Secrétaire Général, les Services de la Commission sont composés d'un Chargé de Mission spécialisé en ingénierie et en sécurité des systèmes, de quatre Juristes ayant des domaines de compétences spécifiques, d'un Informaticien et de deux Agents Administratifs.

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

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

Il a notamment pour missions :

- de s'assurer de la tenue et de la mise à jour du répertoire des traitements ;
- de gérer les consultations du répertoire public ;
- d'élaborer les projets de rapports d'analyses techniques et de délibérations de la Commission ;
- d'élaborer les supports d'informations ;
- de répondre aux questions des responsables de traitements et de les accompagner dans leurs démarches auprès de la Commission ;
- d'informer et de conseiller toute personne intéressée par la protection des informations nominatives ;
- d'instruire les dossiers de plaintes ;
- d'assurer la représentation de la Commission sur le plan international et de participer aux différents travaux des Autorités étrangères de protection des données ;
- d'élaborer les statistiques annuelles de la Commission ;
- d'animer des réunions de sensibilisation ;
- de vérifier si les déclarations, demandes d'avis ou demandes d'autorisation sont complètes au sens de la Loi n° 1.165.

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

03

LA CCIN AUPRÈS DES INSTITUTIONS ET DES ACTEURS DE LA PRINCIPAUTÉ

Bien que le contexte sanitaire de l'année 2020 ait rendu très difficile la tenue de réunion en présentiel, les échanges entre la CCIN et les acteurs de la Principauté n'en ont pas moins été fructueux.

La Commission a été amenée à répondre, dans l'urgence, à de nombreuses sollicitations d'entités essentiellement privées désireuses d'avoir des réponses rapides à leurs préoccupations nouvelles directement liées à la pandémie. Ces échanges font l'objet d'un chapitre dédié : voir Infra : L'activité de la CCIN en lien direct avec la crise sanitaire.

Durant l'année 2020 la CCIN a également poursuivi ses échanges avec les acteurs de la Principauté, sur des thématiques plus « *traditionnelles* ».

Ainsi, dans le cadre de la réalisation de l'Evaluation Nationale des Risques (ENR) en matière de lutte

contre le blanchiment de capitaux menée sous la coordination du SICCFIN, une première réunion s'est tenue courant juillet au cours de laquelle les représentants de la CCIN ont été informés du calendrier prévisionnel de l'ENR. Lors des échanges avec le SICCFIN, la CCIN s'est montrée tout à fait favorable à apporter sa contribution à l'élaboration de « *lignes directrices* » afin que ce document de référence puisse utilement intégrer le volet relatif à la protection des informations nominatives dans ce domaine.

Cette première rencontre a également été l'occasion d'échanger avec le SICCFIN sur l'application de la Loi n° 1.492 du 8 juillet 2020 relative à l'instauration d'un droit au compte, au regard de certaines pratiques de la Place en matière de lutte contre le blanchiment de capitaux.

Au mois de septembre une délégation de la CCIN a été reçue par la Commission de Législation du Conseil National afin d'évoquer les dispositions du projet de Loi tendant à renforcer le dispositif en matière de lutte contre le blanchiment de capitaux, dont la Commission avait été saisie pour avis par le Ministre d'Etat (voir infra : les consultations sur les projets de texte).

Cette réunion a été l'occasion pour la CCIN d'appeler plus particulièrement l'attention des Conseillers Nationaux sur la nécessité d'encadrer plus précisément le périmètre exact des personnes devant faire l'objet des mesures de vigilance en la matière.

Elle a également tenu à rappeler une nouvelle fois l'importance de définir l'ensemble des durées de conservation des informations traitées en matière de lutte contre le blanchiment de capitaux.

De même la création de nouveaux registres (bénéficiaires effectifs, comptes bancaires et coffres forts, ...) a été l'occasion pour elle de réaffirmer l'importance de veiller à un accès strict et clairement défini aux informations appelées à alimenter ces nouveaux registres.

Pour la première fois depuis de nombreuses années une réunion, qui a été particulièrement fructueuse, a eu lieu avec Monsieur le Secrétaire d'Etat à la Justice, également Président du Conseil d'Etat.

L'objectif premier de cette rencontre était d'évoquer les traitements mis en œuvre par les Services Judiciaires et par les Juridictions, tout en ayant à l'esprit que la Loi n° 1.165 relative à la protection des informations nominatives ne s'applique pas aux traitements mis en œuvre par l'Autorité judiciaire pour les procédures diligentées devant les

diverses juridictions, conformément aux standards internationaux applicables en ce domaine.

L'exposé très clair et précis qui a été fait devant la Commission a permis de définir une méthodologie de travail destinée à appréhender de manière pragmatique et efficace les contours des traitements qui seront à lui soumettre pour avis.

L'année 2020 a également donné lieu aux ultimes réunions du Groupe de Travail ad hoc constitué deux ans plus tôt avec les Services de l'Etat afin de définir le futur cadre législatif appelé à remplacer la Loi n° 1.165.

Ces travaux ont donné lieu à l'élaboration d'un projet de Loi dont la CCIN a été officiellement saisie pour avis par le Ministre d'Etat à l'été.

Egalement saisie pour avis de ce projet de texte, Madame le Haut-Commissaire à la Protection des Droits, des Libertés et à la Médiation a souhaité rencontrer la Commission afin d'échanger sur ce projet de Loi, s'agissant plus particulièrement du futur champ de compétence de la nouvelle Autorité appelée à succéder à la CCIN, et des dispositions envisagées en matière de transparence, dans des domaines potentiellement intrusifs pour les personnes concernées.

Fréquemment contactée par la Direction de la Sûreté Publique concernant des problématiques issues de l'utilisation de réseaux sociaux (usurpation d'identité, création de faux comptes nominatifs, ...) des échanges avec les Agents de la Cellule Cybercriminalité de la DSP ont permis de mettre en place une méthodologie de coopération, destinée à intervenir le plus rapidement possible afin que les victimes des ces actes malveillants voient leurs problèmes résolus au plus vite.

Dans ce cadre, un fascicule explicatif de la marche à suivre en cas de difficulté a été réalisé par la DSP, en concertation avec la CCIN, afin d'inviter les victimes à se rapprocher du Secrétariat de la Commission qui, grâce aux connaissances acquises en la matière, parvient rapidement à faire supprimer par les administrateurs des réseaux concernés les propos malveillants ou faux, sans préjudice des poursuites pénales qui pourraient être données à ces actes.

Par ailleurs tout au long de l'année 2020 des réunions régulières ont eu lieu avec les représentants de la Délégation Interministérielle chargée de la Transition Numérique (DITN) afin d'exposer, en amont, les principaux projets avant leur déploiement, dans des domaines aussi variés que la coopération internationale, les logements domaniaux, la e.ambassade, les prestations médicales en faveur des fonctionnaires et agents de l'Etat, la mise en œuvre d'un portail de e.santé, la téléconsultation, etc ..., l'objectif étant d'étoffer les services numériques à disposition des usagers.

Ces échanges toujours très ouverts permettent à la DITN de présenter à la CCIN les grands projets en cours, l'objectif étant que dès la saisine officielle de la Commission les points d'attention aient déjà été identifiés et pris en compte par les Services concernés de l'Etat.

Ces échanges ont bien évidemment vocation à perdurer dans le temps.

A l'initiative de Monsieur le Bâtonnier, des réunions avec les représentants du Conseil de l'Ordre ont permis d'accompagner au plus près les Avocats dans leurs démarches, en tenant bien évidemment compte des spécificités de leur profession et des obligations auxquelles ils sont soumis.

De plus, comme à l'accoutumée, l'année 2020 a donné lieu à de nombreux échanges avec les établissements bancaires et financiers de la Place, toujours désireux de présenter, en amont, à la Commission, les projets d'évolution de leur système d'information, les nouveaux outils de gestion de la relation clientèle qu'ils souhaitent mettre en œuvre, ainsi que des problématiques spécifiques à leurs professions, en lien avec la multiplication des régulations, parfois étrangères, auxquelles ils sont soumis.

En définitive, si l'année 2020 a bien évidemment été fortement impactée par la crise sanitaire, l'organisation de travail mise en place très rapidement a permis la poursuite des relations avec l'ensemble des entités publiques ou privées de la Principauté, désireuses malgré tout de mener à bien des projets initiés de longue date, ou de développer de nouveaux outils en lien direct avec les conséquences de cette crise sanitaire.

04

LE RÉPERTOIRE PUBLIC DES TRAITEMENTS

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

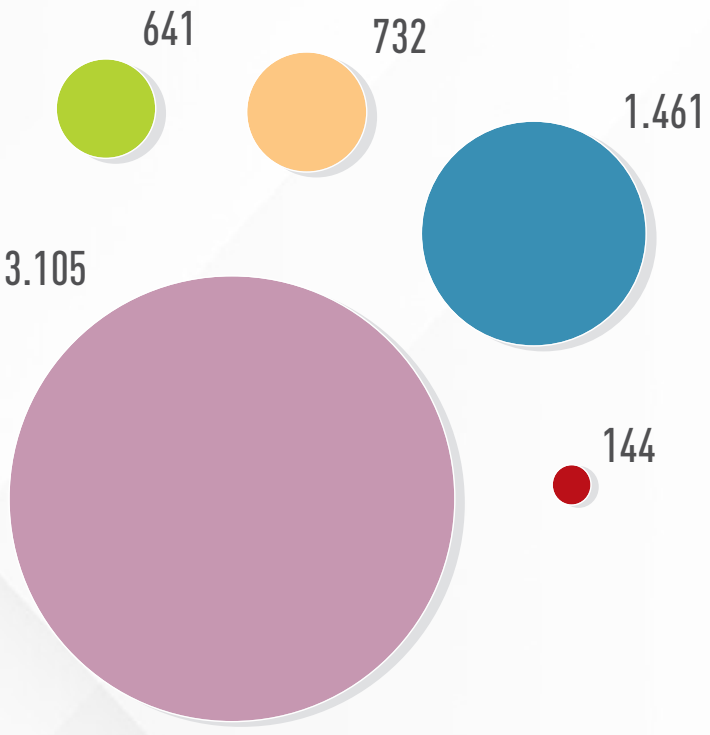
Il peut être consulté au siège de la Commission par toute personne physique ou morale souhaitant s'assurer de l'existence légale d'un traitement automatisé d'informations nominatives.

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

Nombre total de traitements inscrits au répertoire public au 31 décembre 2020

6.083 se répartissant ainsi :

- **641** traitements du secteur public ou assimilé
- **732** traitements ayant fait l'objet d'une autorisation de la Commission
- **1.461** traitements ayant fait l'objet d'une déclaration ordinaire
- **3.105** traitements ayant fait l'objet d'une déclaration simplifiée
- **144** autorisations de transfert vers un Pays ne disposant pas d'un niveau de protection adéquat



Nombre de traitements inscrits annuellement au répertoire par typologie

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

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

Nombre de nouveaux traitements inscrits au répertoire en 2020

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

66

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

72

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

82

traitements ayant fait l'objet d'une déclaration ordinaire

177

traitements ayant fait l'objet d'une déclaration simplifiée

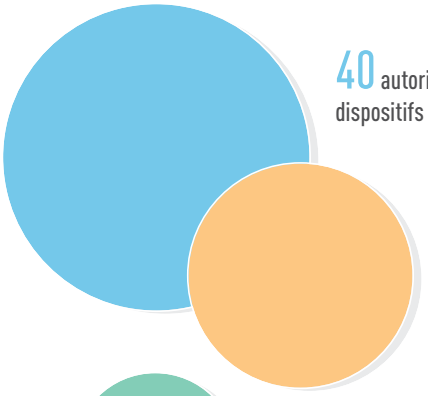
26

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

Nombre de délibérations rendues par la Commission en 2020

Au cours de l'année écoulée, la Commission a rendu **189** délibérations se répartissant ainsi :

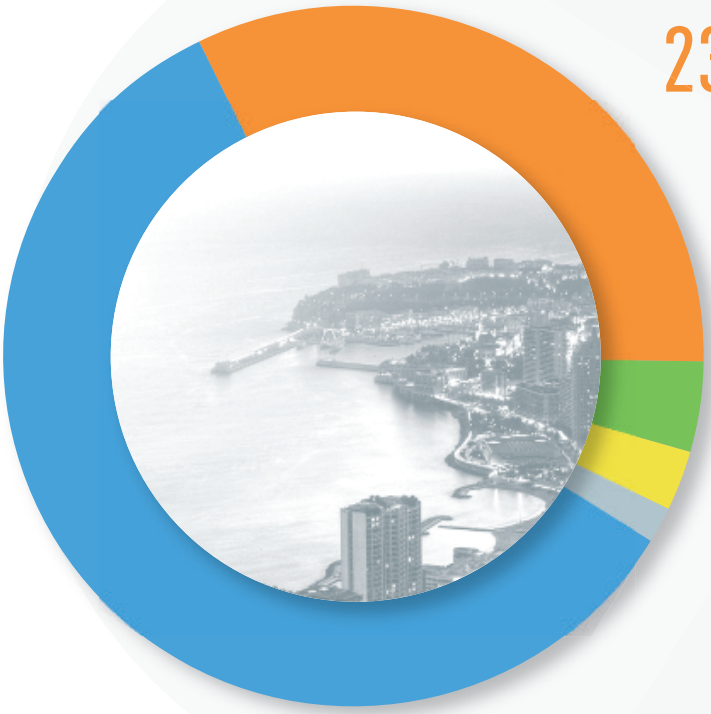
81 autorisant la mise en œuvre ou la modification de traitements :



- **40** autorisations relatives à des dispositifs de vidéosurveillance
- **21** autorisations relatives aux traitements concernant plus spécifiquement le secteur bancaire et assimilé
- **9** autorisations relatives à des dispositifs de contrôle d'accès biométriques ou non
- **3** autorisations relatives aux enregistrements téléphoniques
- **1** autorisation relative à la messagerie électronique
- **2** autorisations relatives aux alertes professionnelles
- **1** autorisation relative à un système de géolocalisation
- **1** autorisation relative à un système de gestion des habilitations
- **1** autorisation relative à la gestion du recrutement et à la vérification de l'intégrité des candidats
- **2** autorisations relatives aux traitements des avocats

1 portant refus d'autorisation

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



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

23 demandes d'avis présentées par le CHPG

3 demandes d'avis présentées par la Mairie de Monaco

2 demandes d'avis présentées par Monaco Telecom

1 demande d'avis présentée par la SMEG

26 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

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

3 Portant sur une mission d'investigation

2 Décisions sur les délais de conservation des informations nominatives prévus par déclaration ordinaire

05

LA CCIN ET LES DROITS DES PERSONNES CONCERNÉES

LES CONSULTATIONS DU RÉPERTOIRE PUBLIC DES TRAITEMENTS

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

Les informations figurant dans ledit répertoire sont les suivantes :

- la date de la déclaration, de la demande d'avis ou de la demande d'autorisation relative à la mise en œuvre d'un traitement ;
- les mentions portées sur celle-ci, à l'exception des mesures prises pour assurer la sécurité du traitement et des informations ;
- la dénomination du Service chargé de l'exploitation du traitement ;
- la date de délivrance du récépissé de la déclaration, de l'avis de la Commission ou de son autorisation ;

- les dates et libellés des modifications apportées aux traitements initiaux ;
- la date de suppression du traitement et celle, lorsqu'il y a lieu, de la radiation de l'inscription.

Au cours de l'année 2020 ce répertoire a été consulté 3 fois, par des Cabinets conseils pour le compte de leurs clients afin de faire le point sur les traitements qui ont déjà fait l'objet de formalités préalables, dans la perspective de poursuivre, ou d'initier, la mise en conformité.

Ceci a concerné au total près de 50 entités privées.

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

LES PLAINTES

19 plaintes ont été adressées à la Commission en 2020, en légère diminution par rapport à l'année précédente au cours de laquelle elle avait été saisie par 24 personnes.

Sur ces 19 plaintes, 3 étaient en lien direct avec la gestion de la crise sanitaire par les employeurs des plaignants (voir chapitre dédié à la crise sanitaire).

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.

10 plaintes ont été reçues en 2020 concernant le droit de suppression, qui a constitué le domaine pour lequel la CCIN a été saisie le plus souvent.

Le droit de suppression

De plus en plus souvent la Commission a à connaître de difficultés rencontrées par des utilisateurs de réseaux sociaux dont les comptes sont piratés et utilisés pour nuire à leur titulaire en publiant des contenus pornographiques, pour procéder à des collectes de fonds en se faisant passer pour des personnalités connues, ou pour faire du chantage en menaçant de publier des contenus totalement inappropriés.

5 cas ont concerné des demandes de « récupération » de comptes piratés, ou de suppression de faux blogs / comptes :

- A 2 reprises la CCIN est intervenue pour faire supprimer des faux blogs à connotation pornographique :
  - Dans le premier cas une personne avait publié des photos d'elle sur un réseau social alors qu'elle était mineure. Des années plus tard, en faisant des recherches à partir de son nom sur

Internet, elle a constaté qu'un blog avait été créé par un inconnu qui avait publié les photos de la plaignante, en prétendant être son petit ami et en tenant des propos totalement inappropriés sur la jeune femme.

- Dans le second cas le plaignant a fait l'objet d'un chantage : un faux blog a été créé à son nom par une personne rencontrée sur un réseau social, le menaçant d'y publier des photos à caractère pédopornographique.

Dans les deux cas la CCIN a obtenu la suppression des blogs en moins de 48 heures.

- 2 de ses interventions ont porté sur la suppression de faux comptes Instagram :

- L'un créé au nom d'une très haute personnalité à des fins de collecte de fonds.

- L'autre en utilisant le nom d'un ancien champion sportif, et qui était utilisé pour poster des commentaires peu élogieux sur d'autres sportifs.

Là aussi ces faux comptes ont été supprimés dans des délais extrêmement brefs.

- 1 plainte a concerné le piratage d'un compte Facebook pour y insérer des contenus pornographiques.

Grace à l'intervention auprès des administrateurs des réseaux sociaux ou sites Internet concernés la CCIN obtient rapidement la suppression des contenus en cause.

Toutefois attention : les contenus / photos publiés en ligne ne disparaissent jamais totalement et peuvent réapparaître des années plus tard pour porter préjudice à leur émetteur initial.

Pour avoir les bons réflexes vous pouvez consulter notre Fiche pratique : Du bon usage des réseaux sociaux sur le site Internet de la CCIN : www.ccin.mc ou à la fin du présent rapport d'activité

5 autres saisines ont concerné des demandes de suppression de contenus en ligne :

- 2 ont porté sur des propos malveillants postés sur Facebook et susceptibles de nuire à l'activité professionnelle des plaignants. Ils ont pu être supprimés rapidement.

- 2 ont concerné des demandes de suppression d'articles à caractère diffamatoire publiés sur un site Internet et accessibles depuis différents moteurs de recherches. Après avoir obtenu le déréférencement de certains articles par Google, les demandes auprès des autres moteurs de recherches sont toujours en cours.

Après des échanges avec les représentants de Google il a été conseillé que les personnes concernées introduisent directement une demande auprès de Google en utilisant le formulaire en ligne relatifs à la suppression de propos diffamatoires : https://support.google.com/legal

- Dans le dernier cas la CCIN a été contactée par la Direction de la Sûreté Publique afin d'obtenir la suppression d'informations relatives à une personne qui se présentait comme étant Notaire à Monaco. Après plusieurs interventions infructueuses pour obtenir la suppression des informations relatives à ce faux Cabinet notarial les représentants de Google ont indiqué à la CCIN que seule la personne à laquelle les fausses informations portent préjudice peut obtenir un déréférencement, ce qui n'était pas le cas en l'espèce. Aussi des courriels ont été adressés directement audit Cabinet. Quelques semaines après il a été constaté que les informations en cause avaient disparu du net, suite à des actions menées également par la DSP.

Le droit d'accès

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

Saisie sur le fondement de ce droit d'accès, la Commission a eu à connaître de la situation d'une personne se présentant comme ayant été adoptée il y a plus de 30 ans par une très haute personnalité de la Principauté, mais n'arrivant pas à le prouver.

A l'appui de sa requête elle avait joint une copie d'un bulletin scolaire qui attesterait de cette adoption.

La CCIN a invité l'intéressé à se rapprocher de la Commune, laquelle était la seule Autorité susceptible de lui fournir les actes attestant de sa prétendue adoption.

Le droit à l'information

En application de l'article 14 de la Loi n° 1.165 « *Les personnes auprès de qui des informations nominatives sont recueillies doivent être averties :*

- *de la finalité du traitement ;*
- *du caractère obligatoire ou facultatif des réponses ;*
- *des conséquences à leur égard d'un défaut de réponse ;*
- *de l'identité des destinataires ou des catégories de destinataires ;*
- *de leurs droits d'opposition, d'accès et de rectification relativement aux informations les concernant ;*
- *de leur droit de s'opposer à l'utilisation pour le compte de tiers, ou à la communication à des tiers d'informations nominatives les concernant à des fins de prospection, notamment commerciale.* »

Ces dispositions ont donné lieu à une saisine de la CCIN, dans le prolongement d'une plainte antérieure relative au traitement des consignés par un établissement de jeux de la Principauté.

Le plaignant a souhaité revenir sur la mesure de consigne dont il avait fait l'objet, considérant qu'elle n'est pas légale. Sur ce point il a été rappelé que ledit traitement avait fait l'objet d'une autorisation de mise en œuvre par la CCIN, et que les mesures de consignes sont régies par les dispositions de la Loi n° 1.103 du 12 juin 1987 relative aux jeux de hasard.

La nouvelle saisine de la Commission a concerné une mention d'information lacunaire portée sur le formulaire de « *notification de consigne* » qui lui a été remis en 2018 lors de la décision de consignation prise à son encontre.

En réponse le plaignant a été informé que dès réception de sa plainte initiale l'attention du responsable de traitement avait été appelée sur la nécessité de compléter les mentions d'informations. Suite à cette démarche il avait été précisé à la Commission que le nécessaire avait été fait.

Par ailleurs la CCIN a également reçu une plainte sans rapport avec la protection des données personnelles, les éléments fournis par le plaignant étant très nombreux, disparates dans leur objet, et imprécis s'agissant des entités exactes objet de sa plainte.

Aussi elle n'a pas été en mesure d'y donner une suite et en a informé la personne à l'origine de sa saisine.

L'exploitation des traitements automatisés d'informations nominatives

La vidéosurveillance

2 plaintes ont concerné des dispositifs de vidéosurveillance exploités par des entités privées, et ont donné lieu à des rappels sur les règles d'exploitation de caméras de vidéosurveillance.

En effet très souvent l'installation de tels dispositifs, qui ont tendance à se multiplier, est faite sans avoir connaissance des réglementations en vigueur (obtention d'une autorisation préalable du Ministre d'Etat et de la CCIN notamment).

Aussi la sensibilisation des responsables de traitement suffit la plupart du temps à régulariser la situation sans qu'il soit nécessaire de procéder à un contrôle sur place.

Ce n'est généralement que lorsque les éléments portés à la connaissance de la CCIN laissent à penser qu'une surveillance permanente des personnes est réalisée, ou que l'implantation des caméras ne respecterait pas leur vie privée qu'il est décidé de procéder à un contrôle sur place.

La vidéoprotection urbaine

La Commission a été saisie par un résident qui s'inquiétait qu'une caméra de vidéoprotection urbaine exploitée par la Direction de la Sûreté Publique et installée à proximité immédiate de son appartement filme l'intérieur de celui-ci.

Ces faits, s'ils étaient avérés, constituant une atteinte manifeste à la vie privée, la Commission a souhaité procéder à un contrôle au sein des locaux de la DSP afin de procéder à une vérification des zones pouvant être filmées par la caméra en cause (voir infra : Les investigations).

Par ailleurs en 2020 la CCIN a été interrogée à de nombreuses reprises par des personnes qui, sans souhaiter la saisir formellement de plaintes, l'ont interrogée pour connaître les règles applicables à tel ou tel domaine, afin de connaître leurs droits ou de faire respecter les bonnes pratiques.

Ceci a concerné des domaines aussi variés que :

- la possibilité pour un syndic de copropriété de demander les nom, prénom, date de naissance et qualification professionnelle de chaque employé intervenant sur un chantier dans les parties privatives des immeubles d'habitation. La CCIN a rappelé qu'en application des dispositions en vigueur, il incombe à l'employeur de s'assurer que ses salariés sont munis de leur carte professionnelle du bâtiment, document qui doit être présenté sur simple demande de l'Inspection du travail.

- la mise en ligne de photos des élèves sur les sites Internet d'établissements scolaires : sur ce point, la CCIN a sensibilisé les administrateurs de ces sites aux bonnes pratiques en la matière, à savoir de ne pas diffuser, sans restriction d'accès, de telles photos, et bien évidemment de recueillir le consentement préalable des responsables légaux à la diffusion des photos des mineurs concernés, en fonction des différents supports.

→ quoi qu'il en soit les mesures mises en œuvre pour limiter la diffusion des photos d'élèves ne doivent pas conduire lesdits élèves à être exclus de toute prise de photo par leur établissement, sauf refus exprès des parents !!!

- la légalité de la transmission par un ancien employeur, d'informations nominatives relatives à un salarié, à une autre entité du même groupe, dans le cadre d'une procédure contentieuse : sur ce point les traitements dont sont issues les informations doivent être légalement mis en œuvre, et les personnes concernées doivent être préalablement informées des catégories de destinataires desdites informations.

→ les informations nominatives doivent être traitées de manière licite, pour une finalité déterminée, au risque de constituer un détournement de finalité constitutif d'une infraction pénale.

LES INVESTIGATIONS

Un contrôle du dispositif de vidéoprotection urbaine

Le contrôle au sein du Poste de Sécurité de la DSP suite à la réception d'une plainte (voir supra Plaintes / vidéoprotection urbaine) a été effectué en fin d'année, et a permis de vérifier que la caméra en question n'était pas orientée par défaut vers l'appartement du plaignant, mais vers la voie publique.

Il a toutefois été constaté qu'en cas de manipulation volontaire des Agents de la DSP sa terrasse et l'intérieur de son domicile pouvaient être filmés.

Cependant, après vérification de l'historique des enregistrements des images issues de cette caméra (30 jours), il a été relevé que tel n'avait pas été le cas durant cette période.

Il convient de relever que l'exploitation du dispositif de vidéoprotection urbaine est encadrée par l'article 5 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, aux termes duquel « *Les opérations de vidéoprotection urbaine de la voie publique sont réalisées de telle sorte qu'elles ne permettent pas la visualisation des images de l'intérieur privatif des immeubles d'habitation* ».

Aussi, des échanges sont intervenus avec les représentants de la DSP, et avec SEM le Ministre d'Etat en sa qualité de responsable de traitement, afin d'envisager la mise en œuvre des mesures adéquates permettant de s'assurer qu'une telle visualisation ne serait effectivement pas possible.

Ces discussions se poursuivront au cours de l'année 2021.

Le plaignant qui avait saisi la Commission de cette question a été avisé du déroulement de ce contrôle et des éléments constatés lors de celui-ci.

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 2020 il a été procédé une vérification auprès de la Direction de la Sûreté Publique. La demande des requérants visait à s'assurer de la prise en compte, dans les traitements mis en œuvre par la DSP, de décisions de justice prononçant l'annulation d'actes d'une procédure d'information.

A l'appui de cette requête étaient joints un Arrêt de la Chambre du Conseil de la Cour d'Appel statuant comme juridiction d'instruction, prononçant cette annulation, ainsi qu'un Arrêt de la Cour de Révision ne la remettant pas en cause.

La question de la portée, et de la prise en compte, de telles décisions a été évoquée avec la Direction des Services Judiciaires.

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

3 vérifications ont été faites dans ce cadre auprès d'établissements bancaires et assimilés.

Enfin en 2020 la Commission a été saisie d'une demande de vérification d'informations en lien avec la maison d'arrêt. En réponse le requérant a été informé de sa faculté d'exercer son droit d'accès direct, et des voies de recours qui lui sont ouvertes à l'encontre des mesures dont il a été l'objet.

06

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

La Commission a été sollicitée par les Services de l'Etat à l'occasion de la mise en œuvre de mesures destinées à gérer, et à endiguer, la pandémie. A cette occasion elle n'a pu que constater, et regretter, soit l'absence de saisine sur des mesures ayant un fort impact en matière de respect de la vie privée, soit des saisines très tardives, alors que les décisions étaient déjà prises par les Services exécutifs de l'Etat, laissant très peu de place à la prise en compte des positions de la CCIN.

Ainsi elle a regretté que les actions et traitements mis en œuvre dans l'urgence n'aient pas été systématiquement assortis des mesures les plus protectrices en matière de données personnelles. En tout état de cause, si les échanges entre le Gouvernement et la Commission ont été d'une totale transparence, cette dernière n'a pu que déplorer les saisines non systématiques, ou en urgence et tardives, sur des sujets aussi sensibles que les données de santé.

La Commission a ainsi pu relever la publication initiale de « *fiches conseils* » relatives au questionnaire de vérification de la santé sur les chantiers, qui ont pu conduire à une collecte, par les employeurs, de données de santé de salariés, sans aucune consultation de sa part.

Elle a pu aussi regretter de n'avoir été que très tardivement saisie sur le projet de Décision Ministérielle relative à la mise en œuvre d'un traitement d'informations nominatives destiné à permettre le suivi de la situation épidémiologique, prise en application de l'article 65 de l'Ordonnance Souveraine n° 6.387 du 9 mai 2017 relative à la mise en œuvre du règlement sanitaire international (2005) en vue de lutter contre la propagation internationale des maladies, sur lequel elle a rendu un avis, en urgence, par délibération n° 2020-084.

Bien entendu, la Commission est solidaire et compréhensive des impératifs qui ont été et qui sont encore ceux du Gouvernement dans une situation inédite de pandémie mondiale. Cette situation a cependant mis en exergue que le droit interne monégasque, s'il est préservé de l'inflation législative que peuvent subir certains pays, ne comporte pas suffisamment en son sein toutes les dispositions nécessaires permettant de répondre clairement et sereinement à la fois aux nécessités de l'urgence sanitaire et aux exigences de préservation des droits des personnes.

DÉCISION MINISTÉRIELLE RELATIVE AU SUIVI DE LA SITUATION ÉPIDÉMIOLOGIQUE

Concernant l'avis de la Commission, rendu par délibération n° 2020-084, sur le projet de Décision Ministérielle permettant le suivi de la situation épidémiologique tel qu'il s'effectuait en 2020, la CCIN a particulièrement attiré l'attention du Gouvernement sur la nécessité de sécuriser les informations objet du traitement, et notamment de maîtriser les accès à ce dernier.

Pour rappel ledit traitement conduit :

- à constituer une base unique centralisée contenant des informations nominatives, dont le quantum est relativement imprécis, sur l'ensemble des nationaux, des résidents, des assurés sociaux et des élèves de la Principauté, par l'alimentation des informations contenues dans les fichiers sources de différents responsables de traitement (SPME, CCSS, etc.) ;

- à collecter sur ladite population des données relatives à la santé.

La Commission a également appelé à une plus grande précision sur la nature des informations pouvant être inscrites dans le traitement de suivi épidémiologique, ce qui a été pris en compte par le Gouvernement.

Elle a également demandé que l'information préalable des personnes soit renforcée, afin de s'assurer que le consentement recueilli soit libre et éclairé, s'agissant plus particulièrement de la campagne de dépistage volontaire à l'attention de la population.

En outre, la Commission s'interrogeait sur la pertinence de garder les informations objets du traitement jusqu'au 21 mai 2021.

Enfin, elle n'a pu que regretter l'absence de prise en compte des cas contacts en droit interne, et de l'encadrement de leur collecte et de leur conservation, qui n'est finalement intervenue qu'en 2021.

MISE EN ŒUVRE DU TRAITEMENT DE SUIVI DE L'ÉVOLUTION DU SARS-COV-2 EN PRINCIPAUTÉ

Postérieurement à l'avis sur le projet de Décision Ministérielle, la Commission a rendu par délibération n° 2020-099 un avis sur le traitement de « *Suivi de l'évolution du SARS-COV-2 de la Principauté* ».

Elle a ainsi considéré qu'en l'état des informations qui lui étaient communiquées à cette date, la durée de conservation jusqu'au 21 mai 2021 n'apparaissait pas justifiée, et que trois mois après la réalisation des tests de dépistage, les informations pourraient être transformées en statistiques anonymes avant suppression.

La Commission a notamment rappelé que :

- les médecins traitants et les représentants légaux des personnes testées doivent être informés de leurs droits ;
- si des recherches de cas contacts sont effectuées, l'anonymat de la personne testée positive doit être préservé en l'absence de consentement de sa part ;
- seuls des personnels de santé doivent être destinataires des informations communiquées par les laboratoires ;
- les personnes concernées doivent être informées de manière conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée, et bénéficier de tout élément leur permettant de consentir librement à la réalisation du test de dépistage.

Elle a également demandé que :

- si un traitement des cas contacts existe, il soit précisé sur le fondement de quelle base légale il est exploité, et qu'il soit soumis à l'avis de la CCIN s'il est automatisé ;
- des précisions soient apportées sur la nature et l'étendue des informations reçues des laboratoires, et qu'une procédure soit adoptée avec eux ;
- les informations des fichiers sources (SPME, CCSS, etc.) soient supprimées dès création de la liste des personnes pouvant bénéficier de la campagne de tests ;
- les personnels de la DRSI, de la DAN, et leurs sous-traitants, n'aient pas accès aux informations objet du traitement ;
- des précisions soient apportées sur les partenariats avec les employeurs privés et publics ; et qu'en tout état de cause, le cadre de la Décision Ministérielle soit respecté.

LES ÉCHANGES AVEC LES ENTITÉS DE LA PRINCIPAUTÉ, EN LIEN AVEC LA CRISE SANITAIRE

Au mois de mai 2020 Monsieur le Conseiller de Gouvernement - Ministre des Affaires Sociales et de la Santé, accompagné de ses équipes et des représentants de la Délégation Interministérielle chargée de la Transition Numérique (DITN), est venu exposer à la Commission les orientations retenues concernant le lancement d'une campagne massive de dépistage par test sérologique. Il a ainsi pu exposer à la Commission les objectifs de cette vaste campagne, destinée à faire un état des lieux de la propagation du virus, et à tenter d'éviter un rebond épidémique.

A également été évoquée l'incrémentation initiale de cette base, par le biais des fichiers « *sources* » exploités par différentes entités (CCSS, SPME, DENJS, Mairie, DSP), ainsi que les accès auxdites données, les mesures mises en place pour préserver leur confidentialité, ainsi que leur durée de conservation.

C'est sur la base de ces échanges qu'a été publiée la Décision Ministérielle du 20 mai 2020 relative à la mise en œuvre du traitement relatif au suivi de la situation épidémiologique de la Principauté.

La gestion de la crise sanitaire a également donné lieu à de nombreuses réunions avec la DITN, et les Directions opérationnelles chacune dans ses domaines de compétence, afin de permettre la réalisation des moyens informatiques nécessaires à l'implémentation de l'ensemble des informations utiles au suivi épidémiologique de la population.

Ainsi, les échanges ont porté sur la mise en exploitation de la « *base de données Covid* » constituée sur le fondement de la Décision Ministérielle précitée, et destinée à l'origine à collecter les résultats de la campagne de dépistage massif par le biais de Tests Rapides d'Orientation Diagnostique (TROD).

Les réunions se sont poursuivies tout au long de l'année, cette base de données ayant été enrichie au fil des mois de nombreuses informations complémentaires, en lien notamment avec la campagne de vaccination.

Dès le début des discussions la Commission a porté une attention toute particulière à la granularité des accès aux informations contenues dans cette base, compte tenu de leur nature, afin de préserver au mieux la vie privée des personnes amenées à y être inscrites.

Dans le cadre de la mise en œuvre des mesures relatives à la gestion de la crise sanitaire le Conseil National, par le biais de son Président et du Président de la Commission Spéciale d'Analyse de la Crise COVID-19 (CSACC), a sollicité la CCIN afin de connaître ses éventuelles observations en la matière.

Aussi la Commission n'a pas manqué de communiquer à la Haute Assemblée, ainsi qu'à SEM le Ministre d'Etat, les éléments de réflexion inspirés par les pratiques et les mesures adoptées au cours de la période écoulée.

Elle a ainsi constaté une insuffisante sensibilisation à la protection des données personnelles en temps de crise, dans l'urgence, et mis l'accent sur la nécessité de déterminer les bases légales adéquates permettant la collecte des informations sensibles que sont les données de santé.

La Commission a de plus souligné certaines pratiques déviantes mises en place par des employeurs que ce soit lors du travail distant (mesures de surveillance constante de l'activité des salariés, obligation d'activation permanente de la webcam à leur domicile), ou à l'occasion de la reprise progressive d'activité (collecte de températures, test de dépistage pour accéder aux locaux).

Dans le prolongement de la transmission de cette note la CSACC a souhaité échanger avec une délégation de la CCIN lors d'une réunion tenue au mois de septembre.

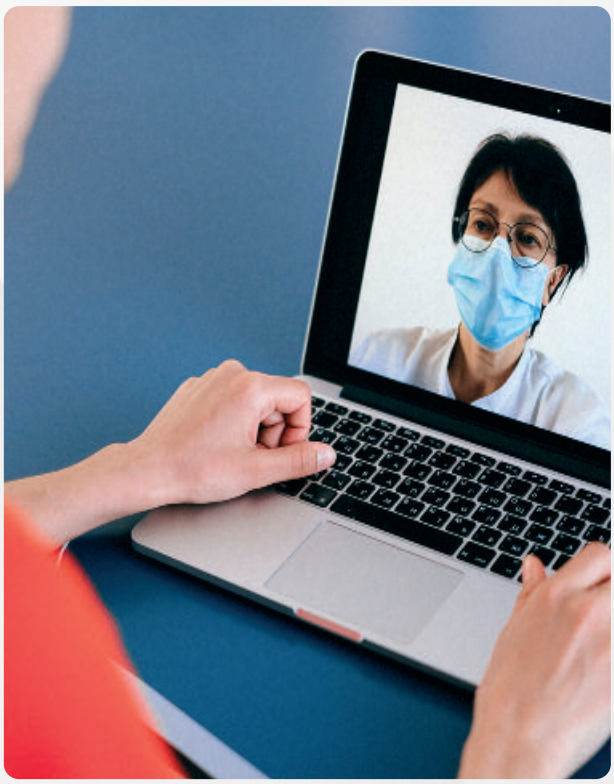
Les élus ont ainsi souhaité recueillir l'avis de la CCIN notamment sur la gestion de la campagne de dépistage, sur les modalités de recueil des « *cas contacts* » pratiqué dans certains restaurants de la Principauté et qui avait donné lieu à une communication de la CCIN sur son site Internet (www.ccin.mc).

De même ont été évoquées la mise en œuvre dans l'urgence, du travail distant lors du confinement, et durant les mois qui ont suivi, donnant lieu à quelques pratiques abusives pour lesquelles la CCIN a dû intervenir auprès des employeurs, ainsi que les modalités de mise en œuvre des prises de température des salariés ou des clients à l'entrée de certains établissements.

A cette occasion le Président de la Commission Spéciale d'Analyse de la Crise COVID-19 a regretté de devoir constater que trop souvent la CCIN n'est pas saisie suffisamment en amont par le Gouvernement s'agissant de surcroit de sujets aussi sensibles en matière de préservation de la vie privée, propos qui ont d'ailleurs été réaffirmés publiquement par la Haute Assemblée.

Des réunions ont également eu lieu avec les représentants du Centre Scientifique de Monaco afin de l'intégrer dans le processus de dépistage de la population, auquel il participe très activement depuis la fin de l'année 2020 grâce à la mise en place de sa nouvelle plateforme de biologie moléculaire à haut débit. L'objectif pour la CCIN était ici de s'assurer de la confidentialité du circuit d'information entre les différents intervenants.

En outre de très nombreux établissements, notamment bancaires, se sont rapprochés de la CCIN afin d'adopter les bonnes pratiques en matière d'accès distants à l'environnement de travail durant les périodes de confinement et de poursuite du télétravail. La Commission a également été fréquemment contactée concernant les mesures de prise de température à l'entrée des locaux, la mise en place de plateformes éducatives pour les élèves, ...



LES RECHERCHES BIOMÉDICALES EN MATIÈRE DE COVID 19

Parmi les 16 études médicales soumises cette année à la Commission pour avis, 3 ont eu pour objet la COVID-19.

C'est ainsi que le 6 avril 2020, la Commission a tenu une réunion exceptionnelle afin d'étudier en urgence la recherche « *Hycovid* » pour laquelle elle a émis un avis favorable. Mise en place par le Centre Hospitalier Universitaire d'Angers, cette étude prospective multicentrique randomisée en double aveugle avait pour objectif principal d'évaluer pendant une durée de 5 mois uniquement l'efficacité de l'hydroxychloroquine versus placebo sur le taux de décès ou de recours à une ventilation invasive chez les patients ayant une infection COVID 19 à haut risque d'aggravation.

Par délibération n° 2020-069 en date du 15 avril 2020, la recherche « *HOME-CoV* », dont l'objectif principal est de démontrer, avec une analyse hiérarchique, que l'implémentation dans les structures d'urgences de critères consensuels de non hospitalisation pour les patients COVID-19 avérés ou probables, par rapport aux pratiques habituelles antérieures, ne majore pas le taux d'évolution défavorable à J7 (critère de sécurité) et diminue le taux d'hospitalisation (critère d'efficacité), a reçu un avis favorable de la Commission.

Mise en œuvre par le Centre Hospitalier Universitaire d'Angers, cette étude devait concerner 50 patients en Principauté.

La Commission a toutefois relevé que la « *Lettre d'information pour le participant* » et le « *Formulaire de consentement pour le patient* » prévoyaient qu'en l'absence d'opposition de sa part, « *des travaux de recherche dans la même thématique pourront être conduits à partir des données collectées pour cette étude* ».

En conséquence, elle a demandé que cette participation ultérieure à des travaux de recherche fasse l'objet d'un consentement séparé, par exemple par le biais d'une case à cocher au sein du formulaire de consentement, afin que le patient puisse effectivement y consentir ou s'y opposer.

Enfin, par délibération n° 2020-110, l'étude ambispective (rétrospective et prospective) « *neothrombocovid* » présentée par le Centre Antoine Lacassagne et dont l'objectif principal est d'évaluer le taux de thromboembolie veineuse à 23 jours au cours d'une infection par COVID-19 chez des patients cancéreux a également reçu un avis favorable à sa mise en œuvre.

La Commission a néanmoins demandé que le document d'information pour l'étude prospective soit complété afin d'indiquer que le patient a le droit de demander, en cas de retrait du consentement, l'effacement des données déjà collectées lorsque celles-ci ne sont plus nécessaires ou s'il n'existe aucune autre exigence légale qui requiert leur conservation.

Elle a également demandé que la participation ultérieure à des travaux de recherche fasse l'objet d'un consentement séparé, par exemple par le biais d'une case à cocher au sein du formulaire de consentement, afin que le patient puisse effectivement y consentir ou s'y opposer.

La Commission a par ailleurs rappelé que si un médecin ou un ARC devait rejoindre la recherche après son début, l'identifiant et le mot de passe devront lui être communiqués par deux canaux distincts et que la communication des données pseudonymisées chiffrées et des clés de déchiffrement doit être effectuée par deux canaux distincts.

POSITION DE LA CCIN AU REGARD DES MESURES SANITAIRES DANS LE CADRE DE LA REPRISE PROGRESSIVE DES ACTIVITÉS À L'ISSUE DU CONFINEMENT

Que ce soit pendant la période de confinement ou durant celle du déconfinement, la CCIN a été interrogée par les employeurs de la place et par des personnes concernées notamment au sujet de la prise de température à l'entrée des lieux de travail, ou des magasins.

Si la CCIN a compris les inquiétudes liées à cette crise sanitaire et les situations exceptionnelles qu'elle peut engendrer, elle a néanmoins estimé que celle-ci ne peut se faire à l'entier détriment des droits et libertés fondamentaux des personnes, notamment au regard du droit au respect de leur vie privée.

Aussi la CCIN a tenu à rappeler la nécessaire précaution qu'il convient d'adopter en matière de données en lien avec la santé.

Elle a donc rappelé que le recours à une prise de température doit correspondre à une exigence particulière et doit se faire de manière proportionnée, conforme aux droits des personnes.

Elle a noté de plus que la levée du confinement a été encadrée par la mise en place de diverses mesures sanitaires (port du masque, utilisation de produits hydro-alcooliques, installation d'écrans de protection, distanciation sanitaire, ...).

Elle a donc demandé :

- qu'il ne soit pas fait recours à la prise de température des salariés sauf cas spécifique le nécessitant ;
- qu'en cas de recours à une telle prise de température des salariés, celle-ci réponde aux critères suivants : une procédure écrite soit établie précisant le seuil de température au-delà duquel l'accès au site n'est pas autorisé ; que ladite procédure soit communiquée aux Instances représentatives du personnel et à l'Inspection du travail ; que les salariés soient informés de ces modalités au préalable ; qu'ils puissent refuser sans conséquence de se soumettre à la prise de température, l'employeur pouvant dès lors accepter le salarié sur le lieu de travail dans les conditions qu'il fixe, ou le renvoyer chez lui sans conséquence juridique ou pécuniaire (salaire maintenu) ; que ces prises de température et la possibilité de refus soient effectuées de manière confidentielle ; qu'aucun relevé de température ne soit conservé ni communiqué ;
- qu'aucun système automatisé ne soit déployé de manière à collecter la température des personnes concernées avant que ces dernières aient été en mesure de consentir ou de refuser la prise de leur température ;
- que l'accès aux clients de magasins ne soit pas subordonné à une prise de température, aucun consentement valable ne pouvant dès lors exister ;

- qu'en cas de recours à un système détectant par caméra le port d'un masque, le système ne collecte à aucun moment de gabarit individualisant les visages des personnes concernées. De plus un tel dispositif ne devrait être mis en place que dans les lieux où le port du masque est obligatoire, et dans lesquels un dispositif moins intrusif peut difficilement être mis en place (surveillance humaine). La Commission a également dû rappeler que les employeurs de la Place ne sont pas autorisés à effectuer des tests ayant pour objectif de déterminer si leurs salariés, ou leurs visiteurs, sont positifs à la COVID-19.

S'agissant en outre de la réouverture des restaurants, et de la mise en place de « *cahiers de rappel* », elle a été contrainte de rappeler que cette pratique, qui ne reposait sur aucune base textuelle, était soumise à la législation relative à la protection des informations nominatives et se devait de respecter pleinement les droits et libertés des personnes désireuses de déjeuner au restaurant.

Ainsi, au fil des semaines, la CCIN a alimenté son site Internet de nouvelles communications et informations afin de répondre aux préoccupations légitimes des personnes qui l'ont contactée.

Tel a été le cas s'agissant de la campagne de dépistage organisée en Principauté à l'été 2020, de la mise en œuvre et de la poursuite du télétravail, de la collecte des coordonnées des personnes se rendant dans un restaurant, de la mise en place de prises de température des salariés à l'entrée des chantiers, et des entreprises. (Ces documents sont disponibles sur le site Internet de la Commission : www.ccin.mc).

LA SOUMISSION DE TRAITEMENTS RÉSULTANT DE LA CRISE SANITAIRE

La modification du dossier médical des patients du CHPG

La Commission a émis un avis favorable sur la mise en œuvre de la modification du traitement automatisé ayant pour finalité « *Gérer les informations médicales du patient afin d'assurer sa prise en charge lors de ses venues au CHPG* », qui permet au responsable de traitement d'ajouter de nouvelles données collectées dans le cadre de l'épidémie de COVID-19 ainsi qu'une nouvelle durée de conservation et un nouveau destinataire pour ces données.

En effet, après avoir relevé que l'article 64 de l'Ordonnance Souveraine n° 6.387 du 9 mai 2017 relative à la mise en œuvre du Règlement Sanitaire International (2005) en vue de lutter contre la propagation internationale des maladies prévoit que « *Les services de l'Etat et de la Commune, les établissements publics, les établissements de santé, les établissements sociaux et médico-sociaux, les services de secours ainsi que tout professionnel de santé sont tenus de signaler immédiatement à la Direction de l'Action Sanitaire les risques imminents pour la santé publique dont ils ont connaissance ainsi que les situations dans lesquelles une présomption sérieuse de risque pour la santé publique leur paraît constituée* », la Commission a considéré que le CHPG pouvait procéder à la collecte de toute donnée de santé nécessaire en cas d'urgence de santé publique de portée internationale reconnue par l'Organisation Mondiale de la Santé et appelant des mesures d'urgence et les transmettre aux Autorités légalement habilitées à les recevoir.

Ces données de santé comprennent entre autres les symptômes évocateurs de la maladie COVID-19 entraînée par le virus SARS-CoV-2 et le résultat positif du test biologique confirmant ou non l'infection par ce virus.

La Commission a également constaté qu'en vertu de l'article premier de la Décision Ministérielle du 23 mars 2020 relative à la déclaration obligatoire de la maladie COVID-19, prise en application de l'article 65 de l'Ordonnance Souveraine n° 6.387 du 9 mai 2017 relative à la mise en œuvre du Règlement Sanitaire International (2005) en vue de lutter contre la propagation internationale des maladies, « *Tout médecin constatant qu'une personne présente les symptômes de la maladie COVID-19 ou en est atteinte est tenu d'en faire la déclaration, dans les plus brefs délais et par tout moyen, à la Direction de l'Action Sanitaire* ».

Elle a en outre pris acte que « *les données seront anonymisées dans un délai d'un an à compter de la collecte* ».

Le Fonds Rouge et Blanc

Dans le cadre du plan de relance de l'activité économique de la Principauté mis en œuvre par le Ministre d'Etat suite à la crise sanitaire liée à la Covid-19, il a été décidé de distribuer aux personnes éligibles (fonctionnaires et agents de l'Etat, personnels relevant de statuts particuliers, certaines catégories de retraités, ...) des bons cadeaux utilisables uniquement dans les commerces situés à Monaco. La Mairie de Monaco et le CHPG se sont également joints à l'opération, ce qui s'est traduit par trois avis favorables de la Commission concernant ces traitements de gestion des bons cadeaux.

Le système fonctionne par le biais d'une application dénommée Carlo. Leur attribution s'effectuait cependant par le biais des traitements des différents responsables de traitement, notamment les traitements de paie et de retraites du Gouvernement, de la Mairie et du CHPG.

Si ces Entités n'ont pas accès à la nature des achats effectués par les bénéficiaires des bons cadeaux, elles devaient cependant connaitre le montant des dépenses effectuées par ces personnes. En effet, l'utilisation des bons cadeaux était limitée dans le temps, sous peine d'être perdus. Il convenait donc que ces Entités ne paient que les sommes effectivement dépensées par les personnes concernées.

La Commission, en ce qui concerne les durées de conservation de ces informations demandées par le Gouvernement de « *40 ans après l'âge légal de la retraite* », les a fixées à 5 ans à compter du versement effectif de la prime, ce délai permettant de résoudre un éventuel litige entre la personne concernée et l'entité ayant délivré ces bons d'achat.

Par ailleurs, de très nombreuses entités, et notamment des établissements bancaires et assimilés, se sont rapprochés des Services de la Commission, en urgence, lors du confinement, afin de valider les mesures de sécurité à mettre en œuvre afin de permettre un accès distant, et sécurisé, à leur SI.

LES PLAINTES EN LIEN AVEC LA COVID-19

Dans un contexte extrêmement tendu du fait de la crise sanitaire et des mesures mises en œuvre pour y faire face, les pratiques instaurées par certains employeurs ont suscité des interrogations, et même parfois de vives craintes, de la part de leurs salariés, qui ont alors saisi la CCIN de 3 plaintes.

La mise en œuvre du travail distant

Si la mise en œuvre du travail distant, le plus souvent en urgence, s'est effectuée la plupart de temps de manière satisfaisante, il n'en demeure pas moins que la CCIN a eu à connaître de préoccupations légitimes de salariés qui ont nécessité une intervention de sa part auprès des employeurs concernés.

L'utilisation de la webcam dans les domiciles des salariés

Ce sujet revêt une acuité toute particulière, certains employeurs ayant demandé à leurs salariés en télétravail d'activer de manière permanente la webcam, à leur domicile, durant les horaires de travail.

Aussi les principes ci-dessous ont été rappelés aux employeurs concernés, et les agissements en cause ont cessé :

Si vous avez fourni des « *webcams* » à vos salariés : afin de préserver la vie privée des salariés et de leur entourage les caméras ne doivent pas être activées de manière permanente, mais uniquement pour des circonstances spécifiques (participation à certaines réunions de travail par visioconférence par exemple). Cependant vos salariés doivent pourvoir refuser d'utiliser la caméra, sauf justification étayée le nécessitant. Dans le cas contraire le recours à la conférence téléphonique constitue une modalité adéquate de participation aux réunions de travail.

Les visioconférences ou les conférences téléphoniques ne doivent pas donner lieu à enregistrements, sauf justification particulière à des fins probatoires par exemple. Si tel est le cas les participants doivent en être préalablement informés.

Des mesures de surveillance de l'activité des salariés

Afin de suivre l'activité des salariés à leur domicile, certains employeurs ont mis en place des tableaux de suivi et de compte rendu d'activité hebdomadaire.

Si de telles pratiques peuvent se concevoir afin d'effectuer un suivi des activités de leurs entités, il n'en demeure pas moins qu'en cas de surveillance de l'activité individuelle des salariés, un formalisme préalable est requis (autorisation de la CCIN, information des salariés, ...).

Là aussi les situations qui ont été portées à la connaissance de la CCIN ont pu être régularisées rapidement.

L'utilisation de la messagerie électronique d'un salarié en son absence

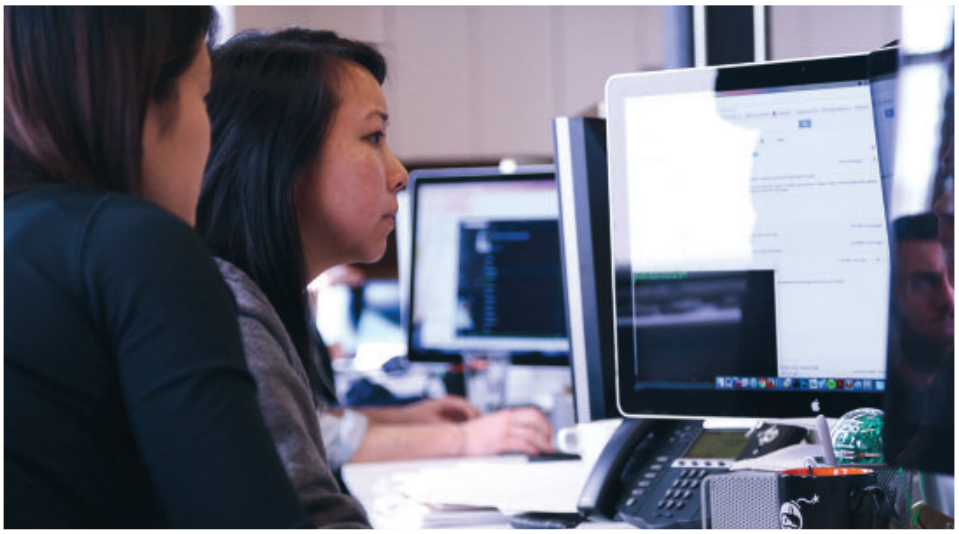
Les problématiques liées aux bonnes pratiques à respecter en matière de messagerie électronique en cas d'absence temporaire, ou de départ définitif, d'un salarié constituent un domaine dont la Commission est souvent saisie.

En l'occurrence elle a été saisie par une salariée ayant constaté que son adresse email nominative professionnelle était utilisée par une autre salariée, lors de la période de confinement.

La Commission s'est immédiatement rapprochée de l'employeur pour lui rappeler les principes en la matière :

- blocage de la messagerie en cas de départ définitif du salarié ;
- information préalable des salariés concernant les règles d'accès et /ou de délégation en cas d'absence ;
- rappel que les messages identifiés comme « *privés* » ne doivent pas être consultés par un tiers ;
- mise en place d'un message automatique de réponse mentionnant l'absence du salarié, ou son départ définitif, et la personne à contacter, ...

07



LES DOSSIERS DU SECTEUR PUBLIC ET ASSIMILE

LA GESTION DE LA TOUR DE CONTRÔLE ET DES LICENCES DES PILOTES MONÉGASQUES PAR LA DIRECTION DE L'AVIATION CIVILE

Conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993, modifiée, la Direction de l'Aviation Civile (la DAC) a soumis à l'avis de la Commission une demande relative à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité la « *Gestion de la tour de contrôle et des licences des pilotes monégasques* ».

La DAC a notamment pour missions de gérer l'espace aérien monégasque et l'héliport, de suivre la navigabilité des aéronefs et la validation des licences des personnels navigants mais également de superviser les exploitants des aéronefs.

Le traitement soumis à l'avis de la Commission concernait plus particulièrement les pilotes de la

Principauté, ainsi que les exploitants d'appareils atterrissant ou décollant de l'héliport de Monaco.

En outre, il a vocation de permettre à la DAC d'enregistrer les vols et tous les paramètres nécessaires à ceux-ci, de gérer les exploitants, les appareils, les types de vols, les villes, les pilotes et leur licence et enfin, de générer automatiquement ou manuellement les factures et d'enregistrer leur règlement.

Ce traitement a reçu l'avis favorable de la Commission, qui a constaté, pour l'édition des factures, la présence de zones permettant d'y inscrire des commentaires libres.

Aussi, outre quelques remarques usuelles, elle a tenu à rappeler que les commentaires pouvant être inscrits dans des « *zones d'observations* » doivent être strictement factuels.

Elle a au surplus fixé, à une durée conforme aux prescriptions légales en la matière, la durée de conservation des données de facturation qui n'était précisée.

LES TRAITEMENTS DE L'INSPECTION DU TRAVAIL

Au cours de l'année 2020, le Ministre d'État a adressé à la Commission plusieurs demandes d'avis portant sur des traitements automatisés d'informations nominatives exploités par le Service de l'Inspection du Travail de la Direction du Travail.

Ce Service est notamment chargé de vérifier la conformité des entreprises monégasques à la Loi sur la durée du travail.

La Direction du Travail a ainsi souhaité mettre à la disposition des entreprises monégasques, des téléservices afin de faciliter les demandes de dérogation qu'elles sont susceptibles d'adresser à l'Inspection du Travail.

Ces derniers avaient respectivement pour finalités :

- « *Demander une dérogation relative aux jours fériés légaux* »,
- « *Demander une dérogation à la durée du travail* »,
- « *Demander une dérogation relative au travail de nuit des femmes salariées* » et,
- « *Demander une dérogation au temps de repos quotidien accordé aux femmes* ».

Le responsable de traitement a justifié la mise en œuvre de ces téléservices par l'existence d'une obligation légale, par la réalisation d'un intérêt légitime consistant à simplifier les démarches des usagers mais également par le consentement des personnes concernées. Il était à cet égard précisé que le consentement de ces dernières est indispensable pour créer un compte sécurisé et accéder à la démarche en ligne.

La Commission a considéré que l'ensemble des traitements soumis à son avis étaient licites et justifiés au regard des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

Elle a toutefois acté le fait que le responsable de traitement collectait en pratique d'autres données en plus de celles renseignées dans sa demande d'avis.

Plus particulièrement, concernant le traitement ayant pour finalité « *Demander une dérogation relative aux jours fériés légaux* », elle a relevé que l'employeur pouvait adjoindre à sa demande de dérogation tout document utile.

De même, s'agissant des traitements ayant pour finalités « *Demander une dérogation à la durée du travail* », « *Demander une dérogation relative au travail de nuit des femmes salariées* » et « *Demander une dérogation au temps de repos quotidien accordé aux femmes* », elle a noté que les plannings de l'ensemble du personnel susceptibles de contenir les informations de tous les salariés de l'entreprise concernée (nom, prénom, horaires) étaient également demandés par le responsable de traitement.

Aussi, conformément aux dispositions de l'article 14 de la Loi n° 1.165 précitée, la Commission a demandé que le Service de l'Inspection du Travail attire l'attention des entreprises sur la nécessité d'informer les salariés de la communication de leurs informations.

LES TRAITEMENTS RELATIFS AU SYSTÈME D'INFORMATION DE L'ETAT

Le Ministre d'Etat a adressé à la Commission des traitements en lien avec le système d'information du Gouvernement ayant pour finalités :

« *Gestion centralisée des accès aux applications du système d'information* » ;

« *Gestion de la politique de filtrage des accès internet* » ;

« *Gestion et analyse des évènements du système d'information* ».

La Commission a principalement effectué ses remarques usuelles et a notamment constaté, pour certains d'entre eux, le recours à des prestataires externes. Elle a ainsi rappelé que ces derniers ne doivent avoir qu'un accès limité au traitement

strictement nécessaire à l'exécution de leur contrat et qu'ils sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement.

En outre, la Commission a formulé des remarques spécifiques à chacun des traitements examinés.

Concernant le traitement ayant pour finalité « *Gestion centralisée des accès aux applications du système d'information* », mis en œuvre pour faciliter l'expérience utilisateur, tout en veillant à la sécurité du système, la Commission s'est contentée de modifier la finalité initiale afin qu'elle soit davantage explicite, comme exigé par la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives.

En outre, le Gouvernement a voulu mettre en place une solution pour éviter que les accès Internet délivrés aux utilisateurs des systèmes d'information du Gouvernement permettent la consultation de sites qui en compromettent la sécurité ou proposant des contenus illicites.

La Commission a relevé lors de l'étude de ce second traitement que le responsable de traitement ne renseignait aucun destinataire des informations bien qu'indiquant conserver les éléments infractionnels dans son système d'information. Elle a, à cet égard, estimé que de telles informations étaient toutefois susceptibles d'être communiquées aux Autorités administratives et judiciaires, agissant dans le cadre de leurs missions légalement conférées.

Enfin, le troisième traitement ayant pour finalité « *Gestion et analyse des évènements du système d'information* » répondait à une volonté de renforcer la sécurisation du système d'information de l'État et de moderniser ses outils de pilotage.

La Commission a constaté que les informations collectées à cet effet étaient transmises, à des fins de stockage, à l'Agence Monégasque de Sécurité Numérique (AMSN). Aussi, elle a demandé

l'exclusion de cette transmission d'autant que l'AMSN était susceptible de lire, à tout moment et en dehors d'alertes avérées, les données transmises. Or, en application des textes, l'AMSN ne pouvait intervenir, qu'a posteriori, pour caractériser une attaque sur les systèmes d'information de l'État. L'AMSN ne pouvait, en revanche, procéder, elle-même, à la sécurisation du système d'information. Cette sécurisation devait être effectuée par des prestataires de services qualifiés en matière de sécurité de système d'information agréés par ses soins. Des modifications textuelles sont depuis intervenues et des précisions sur le rôle de l'AMSN apportées, ce qui a permis quelques mois plus tard de lever les réserves de la Commission.

Enfin, elle a rappelé que les nombreuses interconnexions constatées lors de l'étude du dossier ne doivent pas conduire à créer une surveillance précise, continue et inopportune des utilisateurs du système d'information.

LES OUTILS DE COMMUNICATION DE LA DIRECTION DES SYSTÈMES D'INFORMATION

La DSI (Direction des Systèmes d'Information, anciennement Direction des Réseaux et des Systèmes d'Information devenue la DSI depuis l'entrée en vigueur de l'Ordonnance Souveraine n° 7.996 du 12 mars 2020) a soumis, à l'avis de la Commission, plusieurs traitements automatisés d'informations nominatives concernant la mise en place d'outils destinés à faciliter les échanges avec les fonctionnaires et agents de l'État.

La DSI a ainsi adressé à la Commission 3 traitements ayant pour finalité :

« *Assistance aux utilisateurs par le Centre de service de la DSI* » ;

« *Supervision des appels téléphoniques du Centre de service* » ;

« *Gestion de communication des outils de communication instantanés* ».

Le traitement ayant pour finalité « *Assistance aux utilisateurs par le Centre de Service de la DSI* » avait pour objectif la création d'un outil de génération de tickets de demandes en vue de leur traitement et résolution par le Centre de service.

La Commission a relevé qu'il permettait notamment l'établissement de statistiques à des fins de suivi de qualité de la prestation fournie par le Centre de service. Aussi, elle a rappelé que l'utilisation de données statistiques à des fins de « *contrôle qualité formation* » doit être conforme à l'encadrement prévu dans sa délibération n° 2020-147 du 28 octobre 2020, avec lequel ce traitement est rapproché.

En outre, la Commission a fixé à 6 mois la durée de conservation de ces données et a, par ailleurs, opéré un renvoi à l'une de ses délibérations (délibération n° 2019-144) s'agissant de la conservation des données d'identification électronique. Enfin, elle a demandé à ce que les tickets nominatifs soient conservés en base archive sous couvert de leur anonymisation et, à défaut, qu'ils soient supprimés.

Dans le prolongement du traitement susvisé, l'Administration a souhaité pouvoir superviser les appels téléphoniques reçus par les agents du Centre de service en prévoyant la possibilité d'une écoute en direct des échanges par le Superviseur. L'objectif était de concourir à une efficacité des prestations.

Bien que reconnaissant la légitimité de cette fonctionnalité, la Commission a toutefois rappelé que la mise en œuvre de telles écoutes ne pouvait pas intervenir à l'insu de l'agent concerné et ne pouvait par ailleurs pas conduire à une surveillance permanente et inopportune des agents.

Elle a précisé que l'évaluation de ces derniers ne saurait se faire sur la seule base d'un traitement automatisé appréciant leur aptitude. Enfin, la Commission a une fois de plus émis une réserve concernant la durée de conservation des statistiques nominatives qu'elle a fixée à 6 mois eu égard à l'objectif poursuivi de « *contrôle qualité formation* ».

La DSI s'est également dotée d'outils de communication instantanée. A l'analyse de ce dossier, il est apparu que l'Agence Monégasque de Sécurité Numérique (AMSN) pouvait accéder au traitement en qualité d'Autorité habilitée. La Commission a tenu à rappeler qu'aucun texte ne prévoit un accès permanent des Autorités habilitées aux traitements d'entités tierces, de sorte qu'il ne peut s'agir que d'accès ponctuels faisant suite à des évènements nécessitant leur intervention, dans le cadre de leurs missions légalement conférées. Elle a de plus observé l'existence d'un rapprochement avec un traitement non légalement mis en œuvre et a rappelé que celui-ci devait être régularisé avant qu'un rapprochement puisse être effectif.

MISE EN PLACE PAR LA DSI D'UN SERVICE D'AUTO-PARTAGE AU PROFIT DE SES AGENTS

La DSI a mis en place un service d'auto-partage, dont l'utilisation implique la collecte d'informations nominatives spécifiques, au profit de ses agents et fonctionnaires.

Ce dernier a fait l'objet de quelques remarques.

D'une part, le responsable de traitement a justifié ce traitement par l'existence d'un intérêt légitime mais aussi par le respect d'une obligation légale à laquelle il serait soumis en invoquant la nécessité de pouvoir identifier toute personne qui aurait commis une infraction constatée alors qu'un véhicule était sous sa garde, afin qu'elle en assume les conséquences.

La Commission a considéré que cette justification ne saurait être retenue dans la mesure où aucune disposition n'impose une obligation de dénonciation des personnes verbalisées. Elle a en revanche précisé que la transmission des informations des personnes verbalisées aux autorités requérantes demeurait, quant à elle, licite.

D'autre part, la Commission a relevé l'existence d'un fichier d'état des lieux regroupant un récapitulatif, sur une année glissante, des infractions et des paiements adressés à l'autorité de verbalisation, ainsi qu'une disposition des conditions générales d'utilisation du service précisant que l'Administration avait l'obligation de prendre toutes les mesures d'organisation interne pour lui permettre de révéler à la société d'auto-partage ou aux autorités publiques requérantes, l'identité de l'utilisateur d'un badge de mise à disposition du service.

La Commission a estimé qu'il n'appartenait pas au responsable de traitement de tenir cet état des lieux.

Elle a également demandé que les personnes concernées soient explicitement informées, qu'en cas de verbalisation d'un véhicule conduit par leurs soins, les Autorités requérantes sont destinataires des informations nominatives les concernant. Enfin, elle a sollicité la suppression de la copie du permis de conduire détenue par le responsable de traitement, une fois sa transmission à la société d'auto-partage, cette copie n'étant pas nécessaire au suivi de l'abonnement et à l'utilisation des véhicules.

LA GESTION DES DOSSIERS PRÉCONTENTIEUX ET CONTENTIEUX PAR LA DIRECTION DES AFFAIRES JURIDIQUES

Un traitement ayant pour finalité « *Gestion informatisée des dossiers précontentieux et contentieux visant la coordination et le suivi de la représentation en justice de l'État* » destiné à permettre à la DAJ (Direction des Affaires Juridiques) de préparer et suivre les actions en justice de l'État a été adressé à la Commission.

Parmi les fonctionnalités renseignées, la Commission a constaté l'établissement de statistiques individuelles. Elle a rappelé que celles-ci ne doivent pas conduire à une surveillance continue et inopportune des personnels de la Direction des Affaires Juridiques.

Par ailleurs, concernant l'exercice du droit d'accès des personnes concernées à leurs données, consacré par l'article 15 de la Loi n° 1.165 du 23 décembre 1993 modifiée, la Commission a rappelé que celui-ci ne peut conduire les personnes concernées à accéder directement à l'ensemble des documents qu'il contient, notamment ceux couverts par le secret professionnel des avocats.

Enfin, en termes de durée de conservation, elle a demandé à ce que les logs de connexion soient, non pas conservés 5 jours, comme déclaré par le responsable de traitement, mais 1 an. En effet, une durée de conservation de 5 jours est trop courte eu égard aux impératifs de traçabilité exigés en termes de sécurité.

LE STADE LOUIS II SE DOTE D'UN CONTRÔLE D'ACCÈS PAR BADGES

Le 15 janvier 2020, la Commission a émis un avis favorable à la mise en œuvre par le Ministre d'Etat d'un système de contrôle d'accès de l'accueil du Stade Louis II.

Sont concernés par ce traitement les membres d'associations sportives, les scolaires accompagnés d'un professeur d'EPS, les invités et les VIP.

Dans sa délibération n° 2020-005, la Commission a pris acte des précisions selon lesquelles « *la Direction du Stade Louis II se réserve le droit de ne pas éditer les badges des adhérents d'une Association qui n'aurait pas fait la preuve de sa démarche déclarative auprès de la CCIN* » et a demandé au

responsable de traitement d'indiquer sur le modèle de fichier Excel fourni aux associations que celui-ci ou son contenu soit impérativement sécurisé pour transmission au Stade Louis II.

Elle a considéré en outre que la collecte de la seule année de naissance du détenteur du badge était justifiée afin de prendre en compte les cas d'homonymie.

LA GESTION DES FICHES DESCRIPTIVES DES ÉLÉMENTS DE BÂTIS REMARQUABLES PAR LA DPUM

La Direction de la Prospective, de l'Urbanisme et de la Mobilité (DPUM), qui a notamment la charge d'initier et de suivre différents projets, programmes d'investissement, et études, a reçu le 19 février 2020 un avis favorable de la Commission pour son traitement ayant pour finalité « *Gestion des fiches descriptives des éléments de bâtis remarquables* ».

Celui-ci permet d'identifier et de décrire l'élément de bâti remarquable, de fournir des éléments d'historique, de proposer une valeur patrimoniale et de documenter le bâti à l'aide de photographies.

Outre le nom de l'immeuble, son adresse, son ID BAT, la partie historique présente ainsi un intérêt particulier avec parfois la mention du nom du Commanditaire (permissionnaire) et de l'Architecte s'il s'agit de personnages importants dans l'histoire de la Principauté et de l'immeuble.

La Commission a tenu toutefois à rappeler que les documents d'information à l'intention des architectes et des propriétaires devaient impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Elle a également considéré qu'une procédure relative au droit d'accès par voie électronique devait être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Enfin, la Commission a estimé qu'en application de la Loi n° 1.446 relative à la préservation du patrimoine national, le Conseil du patrimoine était légalement habilité à recevoir communication des informations objet du traitement.

LES TRAITEMENTS DE LA DIRECTION DE L'EDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS

En 2020, la Direction de l'Education Nationale, de la Jeunesse et des Sports (DENJS) a soumis à la Commission deux demandes d'avis concernant la mise en œuvre des traitements permettant notamment de simplifier et de dématérialiser les démarches des représentants légaux des élèves auprès des établissements scolaires.

La DENJS a ainsi déposé un traitement ayant pour finalité « *S'inscrire en classe à horaires aménagés pour la pratique du sport intensif* » qui, par le biais d'un téléservice, permet de demander en ligne une inscription en classe à horaires aménagés pour la pratique du sport intensif, sans avoir à se déplacer et sans autre démarche.

Par délibération n° 2020-164 en date du 18 novembre 2020, ce traitement a reçu un avis favorable de la Commission qui a néanmoins considéré qu'une procédure relative au droit d'accès par voie électronique devrait être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel soit concerné par les informations et qu'en cas de collecte d'une copie d'un document d'identité, sa transmission et son traitement devraient faire l'objet de mesures de protection particulière.

La Commission a en outre demandé que les accès des Directions supports soient restreints au strict besoin d'en connaître et que les interventions de supports soient effectuées selon des modalités définies conformes aux règles de l'art.

Le même jour, la Commission a également émis un avis favorable à la mise en œuvre d'un traitement ayant pour finalité « *Gestion des cantines des établissements scolaires* » qui, par le biais d'un outil dématérialisé, permet aux familles de payer en ligne les repas consommés dans les établissements scolaires publics.

La Commission a cependant considéré qu'en cas de collecte d'une copie d'un document d'identité, sa transmission et son traitement devraient faire l'objet de mesures de protection particulière.

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

Au cours de cette année 2020, la DENJS a par ailleurs déposé une demande d'avis relative à la mise en œuvre d'une modification du traitement ayant pour finalité « *Mise à disposition des élèves collégiens et lycéens d'un outil d'orientation* » qui avait reçu un avis favorable de la Commission en 2019.

Le traitement original mettait en œuvre un « *chatbox* » adossé à Facebook permettant d'aider les élèves scolarisés à Monaco à choisir une orientation qui leur est adaptée. Il nécessitait des transferts d'informations vers les Etats-Unis d'Amérique, pays ne disposant pas d'une législation de protection des informations nominatives jugée d'un niveau de protection adéquat, pour lesquels la DENJS avait reçu une autorisation de la Commission en 2019, sous réserve d'obtenir le recueil du consentement exprès des personnes concernées et/ou de leurs représentants légaux (élèves, parents, ...).

Le traitement tel que modifié conserve comme objectif de « *faire découvrir aux utilisateurs des métiers en adéquation avec leur personnalité et leurs attentes* » et repose sur 3 étapes : 1) collecte des informations auprès de l'utilisateur, 2) traitement algorithmique permettant d'établir un classement des métiers en fonction des informations collectées, 3) restitution des résultats à l'utilisateur.

La DENJS a toutefois souhaité apporter des changements à l'outil proposé, afin que son utilisation se fasse sans association à Facebook ni Chatfuel, via un « *webchat* » et soit ainsi opéré uniquement depuis des pays disposant d'un niveau de protection adéquat en matière de protection des informations nominatives. Aussi, les données ne sont plus accessibles aux destinataires sis aux Etats-Unis d'Amérique et la Commission a ainsi constaté que l'autorisation de transfert ayant pour finalité « *Communication aux Etats-Unis des données des lycéens dans le cadre de la mise à disposition de l'outil d'orientation* » délivrée en 2019 n'avait plus lieu d'être et devait être retirée.

Une autre modification concernait la durée de conservation puisque la DENJS entend désormais conserver les informations objets du traitement 6 ans. Néanmoins, il a été précisé que les informations pouvaient être supprimées à tout instant par les utilisateurs, sauf certaines des informations devant être conservées en respect d'une obligation légale.

Si, par délibération n° 2020-015 en date du 15 janvier 2020, le traitement a reçu un avis favorable, la Commission a néanmoins considéré qu'une procédure relative au droit d'accès par voie électronique devrait être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Par ailleurs, elle a recommandé qu'une sensibilisation à la vie privée en environnement numérique soit effectuée, notamment en ce qui concerne la mise à disposition aux tiers d'un accès au profil de personnalité de l'élève via une url ne requérant pas de mot de passe.

Enfin, la Commission a également rappelé certaines exigences de sécurité.

L'AIDE MÉDICALE DE L'ETAT ET L'AIDE À LA SOUSCRIPTION D'UNE ASSURANCE COMPLÉMENTAIRE SANTÉ

Deux traitements mis en œuvre par Direction de l'Action et de l'Aide Sociales (DASO) ont reçu cette année un avis favorable de la Commission. Ces traitements concernaient respectivement la gestion de l'Aide Médicale de l'Etat (AME) qui permet la prise en charge des frais médicaux et d'hospitalisation à hauteur de 80% ou 100% des tarifs de responsabilité des Caisses Sociales Monégasques, et la gestion de l'aide à la souscription d'une assurance complémentaire santé (ASACS).

La Commission a toutefois assorti ces avis de plusieurs remarques, identiques pour les deux traitements.

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

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

La Commission a par ailleurs demandé que les deux traitements ayant respectivement pour finalité « *Certificats de paiement et listing des bénéficiaires/CGD* » et « *Gestion des contentieux* » dont le responsable de traitement est l'Office de Protection Sociale (OPS) lui soient soumis dans les plus brefs délais.

Concernant la sécurité du traitement, elle a rappelé que toute communication d'informations confidentielles et/ou sensibles par voie électronique devait être sécurisée.

En outre, après avoir constaté que les informations et données étaient enregistrées dans le fichier Excel sans sécurité ni chiffrement, la Commission a demandé que ces informations et données soient chiffrées ou ne soient accessibles que par les personnes ayant à en connaître.

Enfin, elle a fixé la durée de conservation des éléments de traçabilité à 1 an maximum.

LA GESTION DES PRESTATIONS FAMILIALES EN FAVEUR DES TRAVAILLEURS INDÉPENDANTS

Par délibération n° 2020-153, la Commission a émis un avis favorable à la mise en œuvre par la Caisse d'Assurance Maladie, accident et maternité des Travailleurs Indépendants (CAMTI) d'un traitement ayant pour finalité « *Gestion du régime de prestations familiales en faveur des travailleurs indépendants* ».

En effet, suite à la promulgation de la Loi n° 1.493 du 8 juillet 2020 qui institue ce régime en Principauté un formulaire a été adressé par la CAMTI aux travailleurs indépendants afin de recueillir les données utiles pour la constitution des dossiers afin de déterminer les foyers éligibles au versement de prestations familiales et d'en déterminer le type et le montant.

Si la Commission a pu constater que ce traitement s'inscrivait dans le cadre de la mission d'intérêt général de la CAMTI et que les données étaient « *adéquates, pertinentes et non excessives* », elle a cependant relevé à l'étude du dossier qu'un nouveau téléservice avait été créé durant la crise sanitaire Covid 19 en raison des mesures de confinement pour permettre « *aux assurés d'envoyer des documents directement via leur Espace Personnel* ».

Ce traitement n'ayant pas fait l'objet de formalité auprès de la CCIN, la Commission a en conséquence demandé au responsable de traitement de le lui soumettre dans les plus brefs délais.

LES TRAITEMENTS DU CHPG

Comme chaque année désormais, la Commission a eu à se prononcer sur des traitements impliquant le Centre Hospitalier Princesse Grace (CHPG), agissant soit en tant que responsable de traitement, soit en tant que représentant d'un responsable de traitement situé hors de la Principauté.

Ainsi, par délibération n° 2020-008, la Commission a émis un avis favorable à la mise en œuvre d'un traitement ayant pour finalité « *Gestion Electronique de Documents* ». Celui-ci permet au responsable de traitement « *de réduire les coûts de traitement et le temps d'accès aux documents administratifs du CHPG* » grâce entre autres à la numérisation des documents administratifs, au classement et à l'indexation de ces documents et à la traçabilité des actions réalisées.

Enfin, un avis favorable a été émis concernant le traitement ayant pour finalité « *La gestion des dossiers donneurs de sang effectuée par l'EFS* » mis en œuvre par l'Etablissement français du sang dont le CHPG est le représentant en Principauté.

Ledit traitement a été mis en œuvre suite à l'Ordonnance Souveraine n° 7.923 du 14 février 2020 rendant exécutoire l'Accord entre la Principauté de Monaco et le Gouvernement de la

République française relatif à la coopération en matière de transfusion sanguine, signé à Paris le 13 juillet 2017.

Cet Accord a pour objet de préciser le cadre juridique de coopération en matière de transfusion sanguine entre la France et Monaco dans la perspective notamment de fixer les conditions de collaboration et modalités de soutien à l'autosuffisance (monégasque) en produits sanguins, à travers l'organisation de collectes. Les prélèvements/collectes de sang à Monaco seront ainsi réalisés par du personnel du CHPG placé sous la responsabilité fonctionnelle de l'EFS mais les opérations de préparation, de qualification biologique des dons, d'étiquetage, de libération et de distribution des produits sanguins issus des dons réalisés à Monaco seront effectuées par l'EFS (établissement de transfusion sanguine de PACA-Corse en l'occurrence).

Les documents d'information des personnes concernées pas le traitement n'ayant pas été joints à la demande d'avis, la Commission a cependant rappelé que l'information des personnes concernées devait impérativement être conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993. De même, s'agissant de l'exercice du droit d'accès par voie électronique, elle a considéré qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, la Commission a précisé que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Elle a par ailleurs tenu à rappeler que l'Agence de Biomédecine, l'Institut national de veille sanitaire (Santé publique France), l'Institut national de la transfusion sanguine et l'Agence nationale de sécurité des médicaments ne pourraient avoir communication des informations que dans le strict cadre de leurs missions légalement conférées.

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

Le Centre Hospitalier Princesse Grace (CHPG), en tant que représentant sur le territoire monégasque de responsables de traitement situés à l'étranger, a soumis en 2020 à la Commission 16 demandes d'avis relatives à des recherches dans le domaine de la santé.

Les recherches biomédicales

9 des demandes déposées par le CHPG ont concerné des études biomédicales, dont 3 ont été mises en œuvre dans le cadre de l'épidémie de COVID 19 (voir chapitre consacré à la crise sanitaire COVID-19).

Par ailleurs, par délibération n° 2020-009 en date du 15 janvier 2020, la Commission a ainsi émis un avis favorable à la mise en œuvre par le Centre Hospitalier Universitaire de Nice, d'un traitement *ayant pour finalité « Collecter et analyser les données des patients ayant consenti à*

participer à la recherche cherchant à déterminer la durée de portage du virus de la grippe dans les voies aériennes supérieures d'un patient traité par un antiviral ».

Dénommé « *Etude VIRIDAE* », ce traitement porte sur une recherche interventionnelle prospective monocentrique, sans bénéfice individuel direct dont l'objectif principal est de déterminer la durée de portage du virus de la grippe dans les voies aériennes supérieures d'un patient traité par un antiviral.

Cette étude se déroulera uniquement en Principauté de Monaco, au CHPG, où elle sera réalisée sous la responsabilité d'un médecin investigateur exerçant au sein du service Epidémiologie et Hygiène Hospitalière. Elle devrait concerner 100 patients.

Après avoir pris acte de l'avis favorable émis par le Comité consultatif d'éthique en matière de recherche biomédicale, la Commission a cependant demandé que le « *Consentement éclairé* » que signe chaque participant soit modifié afin d'indiquer que les données recueillies avant l'opposition d'un patient pourront être conservées et traitées dans les conditions prévues par la recherche.

Une autre étude intitulée « *PRISTL06562* » mise en œuvre par le laboratoire SONOFI-Aventis, localisé en France a été examinée par la Commission le 6 avril 2020. Elle a pour objectif principal d'évaluer l'efficacité clinique de pristinamycine à la posologie de 2g X 2/j pendant 2 jours puis 1g X 3/j pendant 5 à 7 jours vs amoxicilline 1g X 3/j pendant 7 à 9 jours, 5 à 9 jours après la fin du traitement.

Après avoir remarqué que les deux documents d'information indiquent que les destinataires des données collectées dans le cadre de cette recherche « *peuvent être situés dans un pays ne bénéficiant pas d'un niveau de protection équivalent à celui en vigueur au sein de l'Union européenne* », la Commission a cependant tenu à rappeler que si de tels transferts devaient effectivement avoir lieu, ils devront faire l'objet d'une demande d'autorisation auprès d'elle.

Par ailleurs la recherche biomédicale intitulée « *Trust* », qui a pour objectif principal de déterminer si la stratégie intégrant le doppler transcrânien (TCD) n'est pas inférieure à la prise en charge habituelle en termes d'aggravation neurologique à 3 mois après un traumatisme crânien (TC) sans lésions ou lésions mineures détectées au scanner cérébral initial, a été présentée par le CHU Grenoble-Alpes, représenté à Monaco par le CHPG.

Dans le cadre de l'examen de cette recherche, la Commission a toutefois relevé que la lettre d'information des patients indiquait que la fiche nominative reprenant l'identité du patient (nom, prénom), son adresse mail et son numéro de téléphone constituée pour le suivi téléphonique centralisé à 1 mois et à 3 mois des patients serait détruite à la clôture de la recherche. Or, à l'étude du dossier, il lui est apparu que ces données étaient en réalité détruites à la fin du suivi de chaque patient.

La Commission a donc demandé que la lettre d'information soit modifiée en ce sens.

Lors de sa séance du 15 avril, elle a également émis un avis favorable à la mise en œuvre par l'Intergroupe Francophone du Myélome, basé en France, de l'étude « *CARRISMM* ».

Cette recherche qui doit se dérouler dans plus de 80 centres en France, en Belgique et en Principauté a pour objectif principal d'évaluer le risque annuel estimé à 2 ans de la progression du myélome indolent vers un myélome multiple, en appliquant des nouveaux critères IMWG de 2014.

La Commission a cependant assorti son avis favorable de plusieurs remarques concernant les modalités d'information des patients.

Elle a ainsi demandé que le formulaire de consentement soit modifié afin d'indiquer d'une part que seuls des pays reconnus comme disposant d'un niveau de protection adéquat peuvent être destinataires des informations collectées dans le cadre de cette étude et d'autre part que la conservation des données en vue d'autres recherches que celle faisant l'objet de la demande d'avis soumise, fasse l'objet d'un consentement distinct.

Par ailleurs, la Commission a rappelé que si des transferts vers des pays ne disposant pas d'un niveau de protection adéquat devaient effectivement avoir lieu dans le cadre de cette recherche, ils devront faire l'objet d'une demande d'autorisation auprès d'elle. De même, toute nouvelle recherche à partir des prélèvements et reliquats de prélèvements réalisés dans le cadre de cette étude devra faire l'objet d'une nouvelle demande d'avis auprès d'elle.

Enfin, lors de la réunion du 18 novembre 2020, la Commission a émis deux nouveaux avis favorables.

Le premier concernait l'étude « *SepSIGN* » présenté par BIOMERIEUX dont l'objectif principal est de développer un test sanguin pour prédire l'évolution de l'état clinique des patients ayant une infection et permettre d'améliorer leur prise en charge. Cet avis favorable a été accompagné d'une autorisation de transfert des données à destination du prestataire américain en charge d'héberger et d'analyser les informations, à la condition toutefois que le formulaire de consentement soit modifié afin de préciser que « *Les données collectées seront traitées par une équipe d'expert en bio-statistiques située au Centre Medical Universitaire de Vanderbilt aux Etats-Unis (VMUC)* » pour permettre au patient d'y consentir de manière libre et éclairée.

Le deuxième avis favorable a été donné à l'étude « *FRACTHAL* » mise en œuvre par le Centre Universitaire Hospitalier de Nice. Cette étude doit se dérouler en France et en Principauté de Monaco où elle sera réalisée au CHPG sous la responsabilité d'un médecin investigateur exerçant au sein du service de radiothérapie. Elle devrait concerner 48 patients au total.

Cette étude a pour objectif principal de déterminer le taux de complications ou de déficit neurologique non régressif à 12 mois, en lien avec le traitement, à savoir la thalamotomie radiochirurgicale fractionnée sur accélérateur (3 séances de 50 Gy à l'isocentre) avec détermination de la position de la cible par tractographie.

Lors de l'étude du dossier, la Commission a noté que le « *Consentement éclairé* » que signe chaque patient indiquait que s'il décidait de retirer son consentement, aucune nouvelle donnée ne serait alors collectée mais que « *les données recueillies avant seront conservées et traitées dans les conditions prévues par la recherche, sauf demande expresse* » du patient.

Elle a cependant relevé que le deuxième document d'information, à savoir la « *Notice d'information* », n'évoquait pour sa part que le droit du patient de s'opposer au traitement de ses données personnelles.

La Commission a donc demandé que ce document soit complété afin d'indiquer qu'en cas de retrait du consentement, aucune nouvelle donnée ne sera collectée mais que les données déjà recueillies seront conservées et traitées sauf opposition expresse de sa part.

Les recherches non biomédicales

Parallèlement aux 9 études biomédicales, la Commission s'est également prononcée favorablement sur 7 recherches non biomédicales.

Dans sa délibération n° 2020-006 en date du 15 janvier 2020, la Commission a ainsi émis un avis favorable à la mise en œuvre par GUIDANT EUROPE NV – BOSTON SCIENTIFC de l'étude observationnelle, prospective et multicentrique dénommée « *INTERRUPT - AF* », dont l'objectif principal est d'évaluer les résultats en aigu et à long terme du système de cartographie RYTHMIA™ utilisé conjointement avec les cathéters d'ablation Boston Scientific à irrigation ouverte dans le cadre de primo ablations de la fibrillation auriculaire paroxystique.

Cette recherche se déroule dans environ 25-50 centres aux Etats-Unis, dans la région Asie-Pacifique, en Europe ainsi qu'en Principauté de Monaco où elle est réalisée sous la responsabilité de médecins du CHPG exerçant au sein du service de cardiologie. 41 patients suivis au CHPG sont concernés.

Après avoir noté que les médecins ont la possibilité d'entrer dans le dossier que la « *race et l'origine ethnique ne sont pas divulgués pour ce sujet* », la Commission a estimé que puisque ces données étaient facultatives, leur collecte n'était pas autorisée en Principauté.

Elle a par ailleurs assorti son avis des demandes suivantes concernant les documents d'information préalable :

- que la déclaration de consentement soit modifiée afin de permettre au patient de consentir expressément à l'utilisation ultérieure de ses données ;

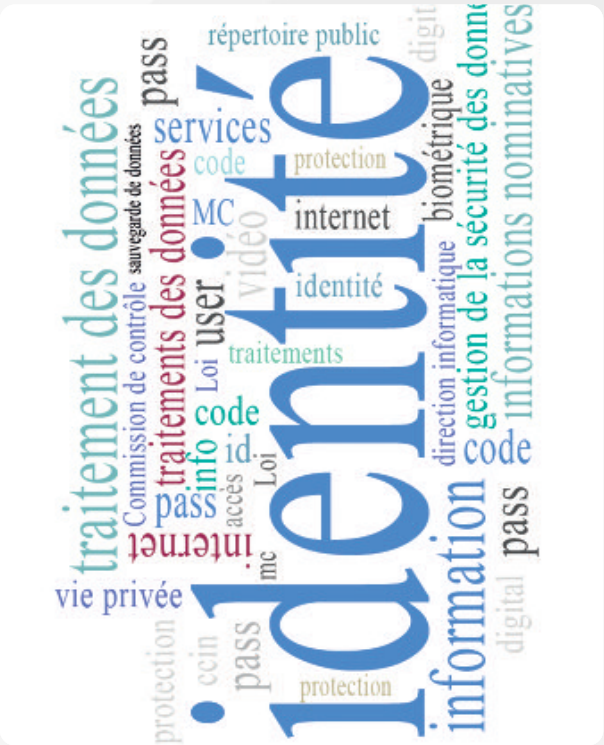
- que le document d'information et la déclaration de consentement soient modifiés afin d'indiquer expressément les transferts des informations vers les Etats-Unis et plus particulièrement les organismes recevant communication des informations ainsi que la finalité desdits transferts afin que le patient puisse y consentir de manière éclairée ;

- que le document d'information soit modifié afin d'expliquer pour quelles raisons les informations ne pourraient être supprimées, particulièrement si cette conservation est liée aux obligations de conformité du responsable de traitement visant à établir la qualité des procédures suivies et des processus mis en place garantissant la fiabilité des résultats de l'étude à l'attention des autorités sanitaires ;

- que la déclaration de consentement soit modifiée afin de mentionner ce qu'il adviendrait des informations collectées en cas de retrait du consentement.

Enfin, la Commission a autorisé concomitamment le transfert des données de santé vers Medidata, le prestataire américain du responsable de traitement chargé de stocker et de mettre en œuvre l'automatisation et la sauvegarde des informations des patients participant à la recherche.

Le mois suivant, lors de sa séance plénière du 19 février 2020, une recherche dénommée « *Profile* » mise en œuvre par Sanofi-Aventis Groupe a été



soumise à l'avis de la Commission. Elle a pour objectif principal de décrire l'efficacité du sarilumab dans la pratique clinique courante chez des patients adultes atteints de polyarthrite rhumatoïde (PR) modérée à sévère sur la base de la variation du score CDAI (Clinical Disease Activity Index, Indice d'activité clinique de maladie) par rapport à la référence, et doit concerner 20 patients suivis au CHPG.

Dans son avis favorable, la Commission a toutefois demandé que la note d'information et le formulaire de consentement soient modifiés afin d'indiquer que les patients sont en réalité uniquement identifiés par un numéro d'identification.

Elle a également demandé que la note d'information soit modifiée et le formulaire de consentement complété afin d'indiquer expressément les organismes recevant communication des informations ainsi que la finalité desdits transferts pour que le patient puisse y consentir de manière éclairée.

La Commission a demandé en outre que la note d'information et le formulaire de consentement

soient modifiés afin d'expliquer pour quelles raisons les informations pourraient ne pas être supprimées, particulièrement si cette conservation est liée aux obligations de conformité du responsable de traitement visant à établir la qualité des procédures suivies et des process mis en place garantissant la fiabilité des résultats de l'étude à l'attention des autorités sanitaires.

Enfin, elle a demandé que si un médecin ou un ARC devait rejoindre la recherche après son début, le login et le mot de passe lui soient communiqués par deux canaux distincts.

Concomitamment, la Commission a autorisé les transferts des informations collectées dans le cadre de cette recherche aux deux prestataires du responsable de traitement, situés respectivement en Inde et aux Etats-Unis, estimant que toutes les conditions étaient réunies pour assurer la confidentialité des données et la sécurité de ces transferts.

Par délibération n° 2020.052 en date du 6 avril 2020, la Commission a émis un avis favorable à la mise en œuvre par le Collège de Pneumologues des Hôpitaux Généraux (CPH), basé en France, de deux études observationnelles, prospectives, multicentriques dénommées « *KBP-2020-CPHG* » pour l'étude principale et « *ESCAP-2020-CPHG* » pour l'étude ancillaire.

L'étude « *KBP-2020-CPHG* » a pour objectif principal d'estimer la mortalité à 1 an et jusqu'à 5 ans après le diagnostic chez les patients ayant un cancer bronchique primitif (CBP) et l'étude « *ESCAP-2020-CPHG* » a pour objectif principal de décrire la stratégie thérapeutique mise en œuvre par les pneumologues des centres hospitaliers durant les trois premières années qui suivent le diagnostic de CBP chez les patients de la cohorte KBP-2020-CPHG.

La Commission a pu constater que la note d'information prévue pour chacune des deux études prévoit que si le patient désire arrêter sa participation à l'étude en question, il peut signaler au médecin investigateur qu'il ne souhaite pas que les données recueillies préalablement à son retrait soient utilisées et que ledit médecin investigateur en avertira le promoteur.

Ces deux documents d'information indiquent également que « *le promoteur peut ne pas faire droit à cette demande afin de ne pas compromettre gravement la réalisation des objectifs de la recherche* ».

La Commission a toutefois relevé que les deux consentements que signe le patient pour chacune des deux études est silencieux sur ce point. Elle a donc demandé que ces deux consentements soient complétés afin que le patient puisse expressément consentir à la conservation éventuelle de ses données en cas de retrait de l'étude.

Sur le plan de la sécurité, elle a rappelé que la communication des données pseudonymisées chiffrées et des clés de déchiffrement devait être effectuée par deux canaux distincts.

Par ailleurs, elle a recommandé que la base de données contenant les informations médicales sur les patients pseudonymisés soit chiffrée.

Le 20 mai 2020, l'étude FORSYA présentée par NOVARTIS Pharma S.A.S. a également reçu un avis favorable de la Commission. Cette recherche qui a pour objectif principal d'évaluer si les signes d'inflammation au moment du démarrage du traitement par sécukinumab sont prédictifs de la poursuite ou non de ce traitement un an plus tard devrait concerner en Principauté 10 patients atteints de spondyloarthrite.

Parmi ses recommandations, la Commission a demandé que le document d'informations et le formulaire de consentement que signe le patient soient modifiés afin d'indiquer si les informations collectées avant le retrait du consentement seront conservées et, dans le cas où ces données ne pourraient être supprimées, d'en expliquer les raisons, particulièrement si cette conservation est liée aux obligations de conformité du responsable de traitement visant à établir la qualité des procédures suivies et des process mis en place garantissant la fiabilité des résultats de l'étude à l'attention des autorités sanitaires.

Elle a par ailleurs demandé que, compte tenu du nombre de patients inclus, le mois de naissance des patients ne soit pas collecté si cette donnée n'est pas un impératif justifié par l'étude. Le mois de naissance pourra toutefois être conservé pour les patients ayant 18 ans l'année de l'inclusion afin de permettre à l'investigateur de démontrer le respect des critères d'inclusion.

Le 1er juillet 2020, la Commission s'est prononcée favorablement à la mise en œuvre de deux nouvelles recherches non biomédicales.

La première présentée par la société FX Solutions, localisée en France, a pour objectif principal l'évaluation en temps réel du taux de révision des systèmes d'épaule à long terme de cette société. Après avoir noté que le formulaire de consentement prévoyait que le patient donne « *la permission de recueillir, de rapporter, de transférer et de traiter les données, au sein de l'Union Européenne, si besoin* » et que « *Dans le cas d'un transfert hors Union Européenne des clauses contractuelles types seront établies afin de protéger la confidentialité* » des données des patients et que ces derniers seront amenés à donner leur accord une nouvelle fois dans cette éventualité, la Commission a tenu à faire les deux rappels suivants :

- que si des communications devaient être effectuées vers des destinataires autres que ceux prévus dans la présente demande d'avis, celle-ci devra être modifiée ;

- qu'en cas de communication vers un pays ne présentant pas un niveau de protection adéquat en matière de données personnelles, une demande de transfert devra lui être soumise.

Par ailleurs, concernant la sécurité du traitement et des informations, elle a rappelé que la communication des données pseudonymisées chiffrées et des clés de déchiffrement doit être effectuée par deux canaux distincts.

La deuxième étude, dénommée « *DEREV* » n'a fait l'objet d'aucune observation particulière. Menée uniquement au sein du service d'urologie du CHPG où elle devrait concerner 500 patients au total, cette recherche a pour objectif principal de comparer la sensibilité du test Xpert® Bladder Cancer Monitor réalisé sur le système GeneXpert à la sensibilité de la cytologie en référence à la cystoscopie (pour les cas négatifs) ou l'histologie (pour les cas positifs) pour la détection de récidive d'une tumeur de la vessie.

Enfin, le 16 décembre 2020, la Commission a émis un avis favorable à la mise en œuvre par l'Association de Recherche Bibliographique et Scientifique pour les Neurosciences, localisée en France, d'une étude observationnelle prospective, descriptive, comparative, monocentrique, dénommée « *MIMP* ».

Celle-ci doit se dérouler au sein du Centre de Gérontologie Clinique Rainier III du CHPG et devrait concerner 10 sujets recrutés parmi les pilotes automobiles retraités venant au CHPG pour la réalisation d'un bilan mémoire ou d'un bilan de commotion.

Pour seule remarque, la Commission a demandé que « *le consentement de participation* » soit complété afin d'indiquer que le patient peut signaler au médecin investigateur qu'il ne souhaite pas que les données déjà recueillies soient traitées et analysées mais que le Promoteur peut ne pas faire droit à cette demande afin de ne pas compromettre gravement la réalisation des objectifs de la recherche.

08

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

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

Dans ce cadre la CCIN a été saisie à 3 reprises de projets de textes, indépendamment des saisines en lien avec la crise sanitaire (voir supra chapitre dédié à la Covid-19)

PROJET DE LOI RELATIVE À LA PROTECTION DES DONNÉES PERSONNELLES

La Commission de Contrôle des Informations Nominatives a été saisie, le 31 juillet 2020, conformément aux dispositions de l'article 2 alinéa 2 de la Loi n°1.165 du 23 décembre 1993, par SEM le Ministre d'Etat d'un projet de Loi visant à réformer le droit monégasque en matière de protection des informations nominatives.

Il est à noter que la rédaction de ce projet de Loi a donné lieu à des réunions très fréquentes entre les Services de la CCIN et ceux de l'Etat, durant plus de deux années, ce dont la Commission n'a pu que se féliciter.

Toutefois, des arbitrages ont *in fine* étaient effectués par les Services de l'Etat, sur lesquels la CCIN a tenu de manière officielle à faire part de ses observations dans le cadre de l'avis qu'elle a adressé à SEM le Ministre d'Etat au mois de novembre 2020.

L'objectif de ce texte est de rapprocher la législation monégasque relative à la protection des informations nominatives de celle des pays membres de l'Union Européenne qui appliquent, depuis le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD).

De même ont également être prises en compte les dispositions de la Convention 108 modernisée, ainsi que celles de la Directive dite Police Justice.

Un tel rapprochement permettrait à la Principauté de pouvoir enfin prétendre à être reconnue, par la Commission européenne, comme un pays disposant d'un niveau de protection adéquat en matière de protection des données personnelles et faciliterait notamment les transferts de données vers Monaco, à l'heure où la Principauté entend développer ses offres en matière numérique.

Dans le cadre de l'avis qu'elle a rendu, la CCIN a entendu insister sur les points qui lui apparaissent essentiels pour obtenir cette reconnaissance, laquelle est en suspens depuis 2012.

De ce fait, elle n'a pu que regretter l'absence de dispositions portant sur certaines catégories de données, telles que notamment les données de santé. Elle a néanmoins pris acte que ces données devraient faire l'objet d'un texte spécifique, sans pour autant avoir de visibilité sur les éventuels encadrements qui seraient apportés à leur traitement.

Dans le cadre de l'examen de ce projet de texte, la Commission a par ailleurs relevé les exclusions prévues du champ de compétence de la future Autorité de Protection des Données Personnelles (APDP) appelée à lui succéder, et sur le peu de visibilité qui serait donnée à ses avis.

En outre, la Commission s'est positionnée sur la question des futurs pouvoirs normatifs de l'APDP, avant d'analyser plus précisément certaines dispositions du projet de texte qui lui a été soumis.

Sur les exclusions du champ de compétence de la future APDP

La Commission n'a pu que regretter l'exclusion, qui est apparue au fil des mois, de certains traitements instaurés par la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale du champ de compétence de la future APDP.

Le projet de texte qui lui a été adressé prévoit en effet de soustraire, de la compétence de la future APDP, le contrôle de la mise en œuvre des traitements utilisant des données issues de l'exploitation de techniques de renseignements prévues aux articles 9 à 15 de la Loi n°1.430.

La Commission a tenu pourtant à rappeler que lors de l'entrée en vigueur de la Loi n° 1.430, aucune exclusion du champ de compétence de la CCIN n'était prévue, le texte faisant au contraire référence à la nécessité de respecter la Loi n° 1.165 relative à la protection des informations nominatives.

Aussi, la Commission a, dans le cadre de son avis, insisté sur le fait qu'il ne serait pas possible d'exclure, du champ de compétence de l'APDP, le contrôle de la mise en œuvre des traitements de renseignements et le respect des droits associés (ex. droit d'accès indirect) sans créer, de manière concomitante, une Autorité administrative indépendante qui en serait chargée.

A défaut, la Principauté contredirait les engagements qu'elle a souscrits au titre de la Convention 108+ du Conseil de l'Europe.

Le texte envisage pareillement une exclusion des traitements issus de l'article 18 de la Loi n°1.430, lequel consacre la notion de secret de sécurité nationale.

Or, cet article 18 associé à d'autres textes, notamment l'Arrêté Ministériel n° 2016-723, permet de couvrir les Opérateurs d'Importance Vitale (« OIV ») par le secret de sécurité nationale, compte tenu de l'acception large à laquelle peut prétendre la notion « *d'intérêts fondamentaux de la Nation* ».

En conséquence, l'exclusion de l'article 18 de la Loi n° 1.430 rendrait difficile voire empêcherait la future APDP de procéder à certaines vérifications au sein des OIV, comme par exemple celles portant sur la sécurité de leur système d'information ou sur l'exercice du droit d'accès indirect dans le cadre de traitements effectués à des fins de lutte contre le blanchiment de capitaux, si les informations concernées devaient être couvertes par le secret de sécurité nationale.

La Commission a, par ailleurs, relevé une évolution quant à la publicité des avis de la future APDP.

Sur la publicité des avis de la future APDP

Le projet de Loi prévoit que la future APDP sera consultée pour avis par le Ministre d'Etat, le Directeur des Services Judiciaires mais également par le Président du Conseil National lors de l'élaboration de projets de texte relatifs à la protection des données à caractère personnel ou lors de la mise en œuvre de traitements de telles données.

La Commission a rappelé qu'à ce jour ses avis ne sont pas tous publiés.

Tel est notamment le cas des avis consultatifs rendus au titre de l'article 2 de la Loi n°1.165, à la suite de la consultation par le Ministre d'Etat « *lors de l'élaboration de mesures législatives ou règlementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement des informations nominatives* ».

De même, pour les traitements relevant de l'article 11 de la Loi n°1.165 (c'est-à-dire, ceux mis en œuvre par les Autorités judiciaires ou administratives intéressant la sécurité publique ou relatifs aux infractions, condamnations ou mesures de sûreté, ou encore ayant pour objet la prévention, la recherche, la constations ou la poursuite des infractions) seul le sens des avis de la CCIN est rendu public.

Si le projet de texte qui lui a été soumis, prévoit certes une évolution en termes de conditions de publication des avis de la future APDP, la Commission a toutefois souligné que ces progrès demeuraient insatisfaisants du point de vue de la transparence.

En effet, dans de nombreux cas, il est prévu que la publication de l'avis soit laissée à l'entière discrétion de l'Autorité consultante.

Pour les traitements qui conserveront des formalités préalables, la Commission a au demeurant déploré qu'il ne soit envisagé qu'une publication du sens de l'avis de l'APDP, ce qui est préjudiciable en termes de transparence vis-à-vis des personnes concernées.

Sur les possibles pouvoirs normatifs de la future APDP

La CCIN est d'autre part revenue sur l'étendue des pouvoirs normatifs de la future APDP dont elle s'était déjà inquiétée, lors des échanges ayant précédé la rédaction du projet de texte.

Elle avait relevé que certains pouvoirs dévolus, par le RGPD, aux Autorités de protection de données, feraient, à Monaco, l'objet d'Arrêtés Ministériels.

Pour toute justification, il lui avait été répondu que doter la future APDP de pouvoirs normatifs serait contraire à la Constitution.

Aussi, quand bien même certains renvois à des Arrêtés Ministériels ont pu disparaitre du projet de texte dont elle a été saisie, la CCIN a néanmoins rappelé, qu'en pratique, il existe des délégations des pouvoirs du Ministre d'Etat dont l'étendue a été confirmée par le Tribunal Suprême.

La Commission a aussi souhaité rappeler qu'elle disposait déjà, antérieurement à l'adoption de la Convention 108+, d'un pouvoir normatif pour délivrer ou retirer des autorisations à certains traitements ou en matière de sanctions, alors même que ceci n'était pas prévu à l'époque par la Convention 108.

Or, ce pouvoir n'a jamais été remis en cause, notamment lorsque la constitutionnalité de la Loi n°1.165 a été examinée par le Tribunal Suprême.

Les remarques générales formulées à l'égard de certaines dispositions du projet de texte

Le projet de texte consacre enfin la disparition d'un grand nombre de formalités préalables qui incombaient jusqu'à présent aux responsables de traitement.

Certaines d'entre elles, touchant les traitements les plus sensibles, devraient cependant demeurer.

Tel devrait être le cas de ceux mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces), ainsi que ceux portant sur des données génétiques ou biométriques ou relatifs à la recherche dans le domaine de la santé.

S'agissant plus particulièrement des traitements dits de police-justice, la CCIN a relevé que la dissémination des dispositions encadrant ces traitements dans différentes dispositions en projet pourrait affecter l'intelligibilité de la norme, sa compréhension, et donc son application.

En outre, la Commission a relevé l'introduction d'un droit à la portabilité des données, tel que prévu par le RGPD, mais a toutefois émis des réserves relatives à son étendue dans le dispositif en projet.

Elle a de la même manière constaté un renforcement des obligations incombant aux responsables de traitement et à leurs sous-traitants notamment en termes de tenue d'un registre des activités de traitement dont elle estime que l'obligation devrait être davantage généralisée compte tenu du tissu économique monégasque, de désignation d'un Délégué à la Protection des Données, d'analyse d'impact ou encore de sécurité des données.

Enfin, elle a estimé qu'il était dommage que le droit des personnes décédées n'ait pas davantage été pris en compte, de même que le traitement de données sensibles effectué par l'Institut Monégasque de la Statistique et des Etudes Economiques, et ce afin d'assoir plus encore ses prérogatives.

PROJET DE LOI RENFORÇANT LE DISPOSITIF DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX, LE FINANCEMENT DU TERRORISME ET LA CORRUPTION

Par sa délibération n° 2020-113 du 1er juillet 2020, la Commission a émis un avis sur la consultation du Ministre d'Etat relative au projet de Loi renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption. Le texte définitif adopté le 23 décembre 2020 a, de nouveau, modifié 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 Loi n° 214 du 27 février 1936 portant révision de la Loi n° 207 du 12 juillet 1935 sur les trusts et la Loi n° 797 du 18 février 1966 relative aux sociétés civiles.

Ce projet de Loi (et la Loi qui lui a succédé) avait pour objectif de renforcer le dispositif monégasque de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption afin d'adopter des mesures équivalentes à celles prises par les Etats membres de l'Union européenne en application de la Directive (UE) 2018/843 du Parlement et du Conseil du 30 mai 2018 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, dite « *5ème Directive* ».

Dans le cadre de son avis, la Commission a, à titre liminaire, rappelé que le dispositif avait été récemment modifié par la Loi n° 1.462 du 28 juin 2018 renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, en intégrant des évolutions de la Directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux ou de financement du terrorisme. La Commission avait rendu son avis relatif au projet de Loi susmentionné par le biais de la délibération n° 2018-033 du 21 février 2018.

Par ailleurs, la Commission a souligné qu'à l'examen des traitements relatifs à la lutte contre

le blanchiment, certains établissements de la Place souhaitaient soumettre aux diligences prévues par la Loi 1.362 du 3 août 2009 leurs employés, ainsi que ceux de leurs fournisseurs et sous-traitants amenés à travailler avec eux.

Aussi, elle a souhaité alerter le Gouvernement sur ces pratiques en rappelant qu'elle n'avait pas autorisé cette typologie de collecte au sein de ces traitements, relevant qu'aucune base légale n'impose de telles vérifications et que seules les personnes expressément visées par la Loi n° 1.362 du 3 août 2009, modifiée, et ses textes d'application sont susceptibles de faire l'objet des diligences qui s'y rapportent.

Concernant les demandes de renseignements du SICCFIN, la Commission a souligné que la réception des demandes de renseignement ne devait pas conduire à l'établissement d'une « *liste noire* » conservée pendant un délai de 5 ans, prorogeable une fois à l'initiative des organismes assujettis. Aussi, elle a considéré que les dispositions permettant la prorogation du délai à l'initiative des établissements assujettis devraient être supprimées afin que la prorogation du délai de 5 ans ne puisse intervenir qu'à la demande du SICCFIN ou du Procureur Général, dans le cadre d'une investigation en cours.

La Commission a également rappelé que certaines remarques formulées dans sa délibération n° 2018-033 étaient toujours d'actualité et les a donc réitérées et développées dans la délibération n° 2020-113 du 1er juillet 2020.

Aussi, concernant le projet de l'article 1er modifiant l'article 1er de la Loi n° 1.362, la Commission a réitéré ses remarques relatives aux précisions des dispositions concernant les personnes soumises à la Loi n° 1.362 afin d'éviter toute notion vague, de garantir la sécurité juridique et d'endiguer tout risque d'interprétations divergentes.

En ce qui concerne le projet d'article 3, modifiant l'article 3 de la Loi n° 1.362, se rapportant aux mesures de vigilance à l'égard de la clientèle, la Commission a renouvelé son interrogation relative à la terminologie de « *sources fiables* » utilisée pour l'identification et l'évaluation des risques LAB-FT-C. Elle a observé à nouveau qu'une « *source fiable* » ne doit pas forcément être une « *source officielle* ». Ainsi, elle a observé qu'un client d'une banque ne figurant sur aucune liste issue d'une source officielle pourrait ne pas pouvoir entrer en relation d'affaires au motif qu'il figure sur une liste issue d'une source non officielle, pourtant considérée comme fiable par la banque. A cet égard, la Commission a réitéré sa recommandation selon laquelle le recours à des listes non-officielles ne puisse pas être de nature à préjudicier les droits des personnes concernées.

Son attention a également été attirée sur l'emploi des termes « *issus de sources fiables et indépendantes* » s'agissant de la documentation permettant l'identification et la vérification du client. A cet égard, la Commission s'est interrogée sur l'adjonction de l'adjectif « *indépendantes* », ce qui laisse à penser que les « *sources fiables* » sus évoquées doivent cette fois-ci être, de plus, indépendantes.

Le projet d'article 10 a inséré le nouvel article 8-1 dans la Loi n° 1.362 relatif au recours par les personnes assujetties à un tiers appartenant au même groupe aux fins d'effectuer les obligations de vigilance et l'appréciation du respect des mesures de vigilance au niveau du groupe. A cet égard, la Commission a considéré que l'application de ces dispositions ne devait pas conduire d'une part à

soustraire les établissements situés en Principauté à leurs obligations, et d'autre part à soumettre les personnes objet de ces diligences à des dispositions étrangères qui seraient moins protectrices de leurs droits.

Par ailleurs, concernant le projet d'article 16 modifiant l'article 14 de la Loi n° 1.362, la Commission a rappelé ses observations relatives aux examens particuliers de toute opération susceptible d'être liée au blanchiment de capitaux. Aussi, elle a réitéré son souhait que la durée de conservation des alertes ne donnant pas lieu à une déclaration de soupçon soit fixée textuellement.

La Commission a également constaté que le projet d'article 23, modifiant l'article 21 de la Loi n° 1.362, relatif aux durées de conservation de la documentation par les personnes et organismes assujettis maintient la locution adverbiale « *au moins* » pouvant conduire à des interprétations multiples et par conséquent à des disparités importantes quant aux durées de conservations appliquées par les

assujettis. Aussi, elle a préconisé le retrait cette locution adverbiale afin de ne laisser subsister aucune possibilité d'interprétation sur la durée de conservation.

L'article 24 en projet relatif au « *registre des bénéficiaires effectifs* » a suscité l'interrogation de la Commission sur la centralisation des demandes auprès du Ministre d'Etat en cas de modifications par voie de déclaration qui devrait être « *notifiée au service du répertoire du commerce et de l'industrie* » et sur l'absence de clarté dans le circuit de l'information. Elle a donc considéré que le texte devait être clarifié, et devait prévoir une liste exhaustive des informations devant figurer sur le registre ainsi qu'une liste des pièces justificatives communiquées à cet effet. Par ailleurs, la Commission a constaté que rien ne venait encadrer les durées de conservations des données relatives à un bénéficiaire économique effectif qui perdrait cette qualité et a souligné qu'une durée de conservation spécifique à ce cas d'espèce devrait être prévue.

De plus, la Commission a relevé que les données du registre sont « *accessibles aux organismes et aux personnes visés aux articles premier et 2* » selon des critères fixés par Ordonnance Souveraine et à toute autre personne intéressée, sans qu'il ne soit fait référence à aucun critère leur fixant des conditions d'accès. Elle a donc relevé que les conditions d'accès doivent être fixées dans toutes les hypothèses et, a constaté que celles-ci ont été intégrées dans une Ordonnance Souveraine n° 8.634, entrée en vigueur le 29 avril 2021 modifiant l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la Loi n° 1.362 du 3 août 2009 et sur laquelle elle s'est prononcée.

L'article 41 en projet, modifiant l'article 44 de la Loi 1.362, a suscité l'inquiétude de la Commission en ce qu'il prévoyait la possibilité de soumettre une déclaration de soupçon même lorsque l'auteur assujetti de la déclaration ne disposait pas d'une

connaissance exacte des faits objets de la déclaration, et même lorsque l'activité ou l'opération projetée n'avait pas été réalisée. Elle s'est inquiétée qu'une telle déclaration soit recevable sur l'unique fondement de la bonne foi de l'assujetti auteur. Aussi, elle a invité le Gouvernement à s'assurer du caractère « *nécessaire dans une société démocratique* » des mesures projetées, au sens de l'article 8-2° de la CESDH.

L'article 49 du projet de Loi, modifiant l'article 51 de la Loi 1.362, porte sur la communication par le SICCFIN à ses homologues étrangers, d'informations en lien avec la LAB-FT-C. A cet égard, la Commission a relevé que le critère de communication des informations « *le traitement des informations communiquées [garantit] un niveau de protection adéquat* » était très restrictif et rendait de facto impossible toute coopération avec certaines cellules de renseignement financier étrangères de pays ne faisant pas partie des pays disposant d'un niveau de protection adéquat.

Aussi, la Commission a estimé qu'en ce qui concerne la coopération avec d'autres Autorités, il conviendrait de prévoir à nouveau un mécanisme de Conventions bilatérales ou d'accords de coopération, comprenant pour les pays non adéquats l'intégration des exigences nécessaires en matière de protection des données personnelles prévues dans la Loi n° 1.165 du 23 décembre 1993, relative à la protection des informations nominatives, modifiée.

L'article 65 du projet de Loi insérait dans la Loi n° 1.362 un nouveau Chapitre IX « *du registre des comptes de paiement, des comptes bancaires et des coffres-forts* » au sein duquel il était prévu à l'article 64-5 que « *le droit d'accès et de rectification aux informations figurant dans le registre des comptes bancaires et des coffres-forts (...) s'exerce auprès de la Commission de Contrôle des Informations Nominatives* ». Néanmoins, La Commission ne comprenait pas pourquoi les personnes concernées n'avaient pas un accès direct aux informations les concernant et elle a estimé, nonobstant les missions d'enquêtes menées par le SICCFIN, que les titulaires devaient pouvoir accéder directement à leurs propres informations. La Commission a pu constater que son avis a été pris en compte à cet égard puisque le droit d'accès s'effectue, conformément à sa suggestion, directement auprès du SICCFIN. Elle a ensuite recommandé que les modalités d'accès des personnes habilitées soient expressément prévues et intégrées dans la Loi notamment concernant leur sécurité et leur traçabilité.

En ce qui concerne les projets d'articles 76 et 79 modifiant la Loi n° 214 du 27 février 1936 portant révision de la Loi n° 207 du 12 juillet 1935 sur les trusts, modifiée, la Commission a demandé que les modalités d'accès au « *registre des trusts* » soient expressément prévues et intégrées dans la Loi notamment concernant leur sécurité et leur traçabilité.

Enfin, concernant le projet d'article 81 créant l'article 14 de la Loi n° 797 du 18 février 1966 relative aux sociétés civiles, modifiée, à l'instar des accès aux autres registres, la Commission a estimé que les accès au registre des sociétés civiles par le SICCFIN devraient être encadrés au sein du dispositif.

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

Par délibération n° 2020-103 du 17 juin 2020, la Commission a émis un nouvel avis sur le projet d'Ordonnance Souveraine relative aux données de santé à caractère personnel produites ou reçues par les professionnels de santé et établissements de santé après que celui-ci ait été modifié afin de prendre en considération les règles de sécurité à appliquer aux systèmes d'informations sensibles édictées par l'Arrêté Ministériel n° 2019-791 du 17 septembre 2019 portant application de l'article 2, a) de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique.

La version définitive de ce texte, l'Ordonnance Souveraine n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé, a été publiée le 13 novembre 2020.

Si la Commission a relevé la prise en compte de certaines des observations et recommandations qu'elle avait émises dans son premier avis en date du 18 septembre 2019, comme par exemple la mise en place de l'obligation de prévenir la CCIN en cas d'incident grave, elle a toutefois regretté l'absence au sein du projet de toute mention énonçant l'obligation d'informer la personne concernée de l'ensemble des mentions d'informations prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

La Commission a par ailleurs estimé que dans un souci de cohérence, une harmonisation des durées entre le délai de conservation du dossier médical prévu par le présent projet d'Ordonnance Souveraine, à savoir 20 ans, et les délais de prescription en matière de responsabilité civile médicale, à savoir 10 ou 30 ans, aurait mérité d'être réalisée.

De même, elle avait préconisé entre autres qu'il soit mentionné que le décès du titulaire du dossier entraîne la clôture dudit dossier qui est ensuite conservé, sous une forme archivée, pour une durée de 10 ans, afin d'en restreindre ses accès.

En ce qui concerne la sécurité du dossier médical, la Commission a insisté sur l'importance de mettre en place des conditions strictes permettant aux médecins d'accéder au dossier médical, telles que la mise en place de codes d'accès, d'un dispositif de verrouillage des postes de travail ou d'une messagerie électronique avec chiffrement des données médicales nominatives.

En outre, elle a recommandé que l'intégrité et la confidentialité des données de santé soient assurées par un chiffrement total ou partiel desdites données selon les cas, que des niveaux d'habilitation différenciés soient créés en fonction des besoins des administrateurs et que cette politique d'habilitation soit tenue à jour et revue régulièrement.

Concomitamment à cet avis, la Commission s'est également prononcée sur le projet d'Arrêté Ministériel d'application de l'Ordonnance Souveraine relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé afin d'encadrer les modalités de qualification des hébergeurs de données de santé à caractère personnel.

C'est ainsi que la version finale du texte, l'Arrêté Ministériel n° 2020-764 du 5 novembre 2020, a, conformément à la remarque de la Commission, remplacé le terme « *niveau élevé* » utilisé dans le projet par celui prévu dans le référentiel d'exigences concernant la qualification des Prestataires d'Informatique en Nuage et d'Hébergement (PINH) publié le 7 décembre 2018 et annexé à l'Arrêté Ministériel n° 2018-1108 du 26 novembre 2018 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique (AMSN), à savoir « *Niveau Avancé* », afin de faire clairement référence au niveau de qualification requis.

Concernant l'audit de surveillance annuel qui doit être réalisé, la Commission a tenu à rappeler dans sa délibération n° 2020-104, qu'avant tout audit, l'organisme de certification ou le prestataire d'audit doit s'assurer que les informations du système à auditer ne contiennent aucune donnée de santé, confidentielle ou sensible, en clair, et qu'en cas d'impossibilité d'auditer le système d'information sans accéder à ces données en clair, des moyens complémentaires de chiffrement devaient impérativement être mis en œuvre.

Elle a également rappelé que tout accès éventuel à des données de santé par l'organisme de certification ou le prestataire d'audit devra obligatoirement être chiffré.

Enfin, la Commission a regretté que les mesures de destruction et d'élimination préconisées ne soient pas modulées en fonction des activités d'hébergeur, telles que prévues par le référentiel PINH.

09

SECTEUR PRIVE : FOCUS SUR DES PROBLÉMATIQUES SPÉCIFIQUES

Lors des séances plénières de la Commission ainsi que dans le cadre des réunions avec les responsables de traitement, quelques problématiques spécifiques ont suscité des discussions au cours de l'année 2020.

LIMITATIONS DU CHAMP D'APPLICATION DES ALERTES PROFESSIONNELLES

Un dispositif d'alerte professionnelle permet à un individu de signaler tout problème survenant sur son lieu de travail, susceptible de mettre en jeu les intérêts ou la responsabilité de l'entreprise ou de l'organisme au sein duquel il travaille, et qui serait contraire à une législation, une réglementation ou aux règles internes de ladite entreprise ou l'organisme, dans un ou plusieurs domaine(s) déterminé(s).

Or, comme la Commission l'avait relevé dans sa délibération n° 2011-73 du 26 septembre 2011

portant recommandation sur les dispositifs d'alerte professionnelle mis en œuvre sur le lieu de travail, la mise en place d'un tel système comprend un certain nombre de dangers qui leur sont inhérents, et notamment :

- le risque de mise en place d'un système organisé de délation professionnelle ou de dénonciation calomnieuse, notamment en cas d'anonymat de la personne dénonciatrice ;
- le risque de disproportion entre le dispositif mis en place et les objectifs poursuivis par l'entreprise ou organisme ;
- 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.

Aussi, afin d'éviter que le périmètre de ces alertes professionnelles ne recouvre des domaines dont les contours sont difficilement appréhendables, la Commission a décidé, dans une délibération en date du 15 janvier 2020, de limiter le champ des alertes professionnelles aux seul domaines suivants :

- actes de corruption (articles 113-2 et suivants du Code Pénal monégasque) ;
- actes de fraudes (articles 331et suivants du Code Pénal monégasque) ;
- actes relatifs au harcèlement et à la violence au travail (Loi n° 1.457 du 12 décembre 2017) ;
- actes relatifs au non-respect de règles d'éthiques professionnelles – protection des clients, régularité des opérations et conflits d'intérêts (Ordonnance Souveraine n° 1.284 du 10 septembre 2007) ;
- actes relatifs au non-respect des règles en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption (Loi n° 1.362 du 3 aout 2009 et Ordonnance Souveraine n° 2.318 du 3 aout 2009, modifiées) ;
- actes relatifs au non-respect des règles en matière de sanctions et d'embargos ;
- actes relatifs au non-respect des règles en matière d'intégrité de marché (Loi n° 1.338 du 7 septembre 2007 sur les activités financières) ;
- actes relatifs au non-respect des règles relatives à la protection des données nominatives (Loi n° 1.165 du 23 décembre 1993, modifiée).

LES PRINCIPES APPLICABLES EN MATIÈRE DE RÉPONSE À UN DROIT D'ACCÈS

Les articles 13 et 15 de la Loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives octroient à toute personne justifiant de son identité le droit d'accéder aux informations personnelles collectées le concernant.

Les principes ci-dessous ont ainsi vocation à aider les responsables de traitement confrontés à une demande de droit d'accès.

Sur l'identité de la personne qui exerce une demande de droit d'accès

Sur la personne pouvant faire la demande

Conformément aux articles 13 et 15 de la Loi n° 1.165 du 23 décembre 1993, modifiée, toute personne physique qui en fait la demande a le droit d'obtenir la confirmation que des données la concernant sont collectées et traitées et peut obtenir communication desdites données. Elle peut également demander que ces informations soient modifiées s'il y a lieu.

Une personne peut ainsi s'adresser à son employeur pour accéder aux informations la concernant détenues par le Service des Ressources Humaines, à son médecin pour avoir une copie des données de son dossier médical, ou bien encore à une administration pour savoir lesquelles de ses données personnelles sont collectées et à quelles fins.

Ce droit d'accès est toutefois limité par le respect du droit des tiers. Une personne ne peut ainsi avoir accès qu'aux seules données la concernant. Elle ne peut donc demander à obtenir les informations détenues sur son conjoint ou sur un collègue de travail.

L'article 13 de la Loi n° 1.165 du 23 décembre, modifiée, prévoit néanmoins un droit d'accès aux informations concernant les personnes décédées. Sous réserve des 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 le droit d'accès aux informations concernant cette personne.

Le droit d'accès ne peut pas porter atteinte au secret des affaires ou à la propriété intellectuelle.

Enfin, la personne concernée par le traitement peut donner un mandat à une personne de son choix afin que celle-ci exerce le droit d'accès à sa place. Pour ce faire, elle devra fournir à la personne la représentant un courrier indiquant l'identité du mandant (le demandeur), l'objet du mandat (l'exercice du droit d'accès) et l'identité du mandataire (le représentant du demandeur).

De même, ce droit d'accès peut être exercé par les détenteurs de l'autorité parentale pour les mineurs et par les tuteurs pour les incapables majeurs.

Sur les justificatifs d'identité à demander

Pour toute demande d'accès, la personne concernée doit pouvoir justifier de son identité.

Lorsqu'un mandat est donné, le mandataire doit justifier de son identité et de celle du demandeur.

Cette justification peut intervenir par tout moyen. Toutefois, le principe est que sauf en cas de doute raisonnable (par exemple, en cas de suspicion d'usurpation d'identité ou de piratage de compte), **la pièce d'identité ne doit pas être demandée.** Seulement si le doute est réel, le responsable de traitement peut alors demander à la personne concernée de joindre à sa demande une photocopie de sa pièce d'identité.

A cet égard, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans la délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels, notamment en ce qui concerne la durée de conservation, les personnes ayant accès aux informations, les destinataires, la confidentialité, le format des copies transmises (**en noir et blanc, et barrée**) et la sécurisation des accès auxdits documents.

Dans la majorité des cas, la vérification de l'identité de la personne peut tout simplement s'effectuer par la demande d'informations supplémentaires, telles que le numéro client du demandeur ou des éléments permettant d'identifier des abonnés à un service.

De même, le fait pour la personne concernée de se connecter à un espace ouvert par le responsable de traitement auquel elle s'est préalablement identifiée, peut être suffisant pour établir son identité.

Il appartient au responsable de traitement de mettre en place des niveaux de vérification adaptés à la nature de la demande et de la sensibilité des informations traitées.

Sur la réponse à une demande de droit d'accès

Sur le contenu de la réponse à un droit d'accès

Après avoir vérifié l'identité de l'interlocuteur, le responsable de traitement ou son représentant doit confirmer au demandeur si des informations le concernant sont ou non traitées. Il sera ainsi tenu de transmettre les renseignements relatifs :

- à la finalité du ou des traitement(s) exploité(s) ;
- aux différentes catégories d'informations enregistrées par traitement ;
- aux divers destinataires auxquels sont transmises les données par traitement ;
- à la durée de conservation des données ou les critères qui déterminent cette durée.

Ces informations devront être communiquées dans un **format compréhensible**, à savoir sous une forme écrite, non codée et conforme au contenu des enregistrements.

Il arrive toutefois que certaines demandes concernent l'ensemble des données traitées par un responsable de traitement, et ainsi un très grand nombre d'informations. Le responsable de traitement peut alors demander à la personne concernée de préciser sa demande de droit d'accès (par exemple, sur quelles données ou quelles opérations de traitement porte la demande).

Si après précision, la demande porte sur l'ensemble des données collectées, le responsable de traitement peut obtenir un délai supplémentaire raisonnable pour y répondre.

En outre, afin de protéger les tiers, le responsable de traitement doit masquer, dans le contenu de sa réponse, l'identité de ces tiers ou des éléments permettant indirectement de les identifier.

Sur les modalités de réponse à un droit d'accès

L'article 15 de la Loi n° 1.165 du 23 décembre 1993 dispose que « *Sauf dispositions législatives*

particulières, il doit être procédé à la communication dans le mois suivant la réception de la demande », sauf cas de demande de délai supplémentaire.

Un responsable de traitement ou son représentant doit en conséquence mettre en place les mesures nécessaires pour que toute personne qui le souhaite puisse exercer son droit d'accès (article 15) et recevoir une réponse dans le mois qui suit.

Une telle obligation implique que le responsable de traitement prévoie :

- **des modalités pratiques** (formulaire, coordonnées) pour exercer facilement le droit d'accès ;
- **un parcours interne efficace** au sein de l'entité pour le traitement des demandes de droit d'accès. Cela nécessite la mise en place de procédures en interne permettant de remonter lesdites demandes au bon interlocuteur afin d'être en mesure de les traiter dans les délais impartis ;
- **des modalités de réponse auprès des personnes concernées qui soient compréhensibles, accessibles, formulées en des termes clairs et simples.**

Si le responsable de traitement estime toutefois que la demande est abusive car la personne concernée en adresse beaucoup dans des délais rapprochés ou régulièrement sur des sujets différents, il peut saisir le Président de la Commission de Contrôle des Informations Nominatives pour lui demander un délai de réponse supérieur à un mois ou pour lui demander une dispense de réponse.

Les modalités de réponse peuvent différer en fonction de la façon dont la personne concernée a exercé son droit d'accès.

Ainsi, lorsque la demande de droit d'accès est effectuée sur place et que le responsable de traitement ne peut pas répondre immédiatement, il devra remettre au demandeur un avis de réception de la demande daté et signé.

S'agissant de l'exercice du droit d'accès par voie électronique, le responsable de traitement doit tout d'abord s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations puis ensuite s'assurer que la transmission des informations demandées est faîte de manière sécurisée.

Lorsque la demande de droit d'accès s'exerce par voie postale, il est conseillé d'y répondre par courrier recommandé avec accusé de réception.

Enfin, il est possible de remettre à la personne concernée un support numérique contenant les informations demandées. Afin de protéger les données contenues sur ce support, il est envisageable de les chiffrer et de communiquer à la personne concernée le code de déchiffrement oralement ou par un autre moyen (SMS, courriel, etc.).

Sur la conservation des demandes de droit d'accès

Certains responsables de traitement conservent les demandes de droit d'accès ainsi que, parfois les documents d'identité collectés dans le cadre de ces demandes.

A cet égard, la Commission considère que ces demandes et documents ne doivent pas être conservés plus de 3 ans conformément à l'article 13 du Code de Procédure Pénale.

TRAITEMENT MÉTIER DES AVOCATS : GESTION DE LA CLIENTÈLE DANS LE CADRE DES ACTIVITÉS DE CONSEIL, DE REPRÉSENTATION ET DE DÉFENSE

Au cours de l'année 2020, la Commission a été destinatrice de plusieurs formalités ayant trait au traitement métier des Avocats « *Gestion de la clientèle dans le cadre des activités de conseil, de représentation et de défense* ».

Ces dernières, qui s'inscrivent dans le cadre d'échanges intervenus entre le Secrétariat Général de la Commission et le Bâtonnier de l'Ordre des Avocats en exercice, ont toutes obtenu une autorisation de mise en œuvre.

En effet, les informations nominatives traitées, par les Avocats, dans le cadre de leurs activités de conseil et de défense peuvent contenir des soupçons d'activités illicites, des infractions et des mesures de sûreté et comporter par ailleurs des données biométriques nécessaires au contrôle de l'identité des personnes.

De ce fait, le traitement métier des Avocats relève du régime d'autorisation préalable de la Commission, régit par l'article 11-1 de la Loi n°1.165 du 23 décembre 1993 modifiée.

Il répond principalement aux finalités suivantes :

- La gestion des dossiers clients dans le cadre des missions de conseil, de défense et de représentation devant les Cours et les Tribunaux ;
- La préparation et la rédaction des plaidoiries ;
- La rédaction de consultations et d'actes juridiques et judiciaires ;
- La gestion des coordonnées de confrères et, plus généralement, de toute personne intervenant dans une procédure ;
- La gestion des audiences et des agendas ;
- La gestion des informations clients aux fins d'anticiper les conflits d'intérêts ;
- La communication des pièces de manière sécurisée ; et enfin ;
- L'archivage à des fins probatoires.

Ce traitement a, le plus souvent, été justifié, tant par le mandat liant l'Avocat à son client, que par la Loi n° 1.047 du 28 juillet 1982 modifiée sur l'exercice des professions d'Avocats-Défenseurs et d'Avocats ou encore, par l'intérêt légitime des personnes concernées de recourir aux services d'un Avocat.

A la lumière de ces justifications, la Commission a considéré ce traitement comme étant licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

Les informations nominatives collectées pouvant être des données sensibles la Commission a pris bonne note de ce que seules les informations « sensibles » (données médicales, ...) strictement nécessaires à la défense des intérêts des clients sont traitées par les responsables de traitement.

La Commission a néanmoins insisté sur l'importance de limiter l'accès aux informations aux seules personnes qui, dans le cadre de leurs attributions, peuvent légitimement en avoir connaissance au regard de la finalité du traitement.

Pour rappel, la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit être communiquée à la Commission à première réquisition.

Enfin, d'un point de vue de la sécurité des informations traitées, la Commission a eu l'occasion de rappeler que le responsable de traitement doit prendre toutes les mesures utiles pour préserver la sécurité des informations en protégeant individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé, les comptes des utilisateurs et des administrateurs et en s'assurant, par ailleurs, que les communications électroniques soient sécurisées, en tenant compte de la nature des informations transmises.

10

LA CCIN SUR LE TERRAIN

Afin de connaître les attentes, les projets, les interrogations des responsables de traitement, sur la protection des informations nominatives, les Agents de la CCIN se tiennent à l'écoute des acteurs économiques et publics.

NIVEAU NATIONAL ET REGIONAL

14ème Université des DPO organisée par l'AFCDP à Paris le 14 janvier 2020

Comme les années précédentes le Secrétaire Général de la CCIN a été convié à participer à l'Université annuelle des DPO organisée à Paris le 14 janvier 2020 par l'AFCDP. Cette Université qui a accueilli plus de 1.000 participants a été une nouvelle fois l'occasion de partager sur les retours d'expériences des professionnels de la protection des données personnelles.

Au cours de son intervention la Présidente de la CNIL a fait part des nombreuses actions menées par ses Services afin de poursuivre l'accompagnement dans l'application des nouvelles obligations

qui incombent aux responsables de traitements depuis l'application du RGPD, ainsi que sur les nouveaux droits dont bénéficient désormais les personnes concernées. Dans ce cadre elle a annoncé la tenue d'un Colloque sur la portabilité des données afin que chacun puisse apprécier les contours exacts de cette nouvelle notion.

Par ailleurs le Chef de l'Unité « *protection des données* » à la Direction Générale de la justice et des consommateurs de la Commission européenne a mis l'accent sur le travail d'uniformisation réalisé par les Services de la Commission auprès de tous les Etats Membres afin que l'application du RGPD se fasse de manière identique dans chacun des pays. A titre indicatif il a notamment précisé que des travaux étaient en cours afin d'harmoniser l'application de la notion d' « *intérêt légitime* » dont se prévalent les responsables de traitement pour mettre en œuvre un traitement de données personnelles.

Participation au Forum International de la Cybersécurité

Fin janvier, deux agents du Secrétariat Général se sont déplacés à Lille pour assister à la 12ème édition du Forum International de la Cybersécurité (FIC) qui, avec plus de 12 500 participants, dont près de 2500 visiteurs internationaux, et pour la première fois une ouverture sur trois jours, est l'un des événements de référence en Europe en matière de sécurité et de confiance numérique.

Pendant trois jours, ils ont ainsi pu participer à des conférences, débats et autres tables rondes autour du thème « « *replacer l'humain au cœur de la cybersécurité » afin de réconcilier sécurité et expérience utilisateur.* »

Ce fut également l'occasion pour eux de rencontrer les acteurs majeurs de la confiance numérique, des éditeurs de solutions et hackeurs éthiques aux enquêteurs de la Gendarmerie et autres Autorités publiques (ministère de l'Intérieur, ANSSI, CNIL, ministère des Armées, ministère de l'Europe et des Affaires étrangères...).

De très nombreuses entreprises aux activités aussi diverses que l'énergie, le transport, l'industrie ou la grande distribution étaient également présentes témoignant des craintes que représentent désormais les menaces informatiques pour les décideurs privés. « *Toutes les entreprises se sont déjà faites attaquer ou le seront un jour. Il n'y a pas de honte à avoir* » a ainsi souligné Guillaume Tissier, Président de CEIS. « *Pour ces entreprises, la cybersécurité est non seulement une exigence opérationnelle mais également un véritable avantage business et marketing* ».

Pour combattre toutes les formes de cybercriminalité, des mesures concrètes ont été annoncées au FIC 2020 dont la création prochaine de 9 antennes régionales du Centre de lutte contre les criminalités numériques (C3N) et de la plateforme Thésée pour lutter contre les escroqueries en ligne (90 000 personnes venues chercher de l'assistance sur la plateforme cybermalveillance.gouv.fr en 2019).

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

Réunion à Berne (Suisse) sur l'impact du RGPD sur les pays tiers à l'Union européenne

Un an après avoir reçu des représentants des Autorités de protection des données suisse et andorrane, plusieurs membres du Secrétariat Général de la CCIN se sont rendus à Berne (Suisse) en février 2020, afin de continuer les discussions engagées sur les conséquences de l'application du RGPD pour les responsables de traitement des

pays tiers à l'Union européenne. Outre la Suisse, l'Albanie et Jersey ont également participé à cette seconde réunion dont le but était d'identifier les problématiques rencontrées par les responsables de traitement et de proposer des actions communes auprès des Instances européennes.

Même si elle n'est pas membre de l'Union européenne, la Principauté de Monaco est en effet impactée par le RGPD en vertu des critères d'établissement et de ciblage prévus à l'article 3 de ce texte sur le champ d'application territorial.

Ainsi, en vertu du critère d'établissement, un responsable de traitement ou sous-traitant basé à Monaco mais ayant un établissement dans l'Union européenne, est soumis au RGPD dans le cadre des activités de cet établissement, que le traitement ait lieu ou non dans l'Union. De même, un sous-traitant travaillant pour un responsable de traitement établi dans l'Union européenne, doit respecter les nouvelles obligations du sous-traitant en vertu du RGPD.

En vertu du critère de ciblage, dès lors qu'un responsable de traitement (ou bien un sous-traitant) situé à Monaco offre des biens ou des services à des personnes se trouvant au sein de l'Union européenne, il devra respecter les nouvelles obligations du RGPD. Par ailleurs, un responsable de traitement (ou bien un sous-traitant) situé à Monaco devra également respecter les nouvelles obligations du RGPD dès lors qu'il traite des données personnelles dans un but de suivi du comportement des personnes concernées au sein de l'Union européenne.

A été évoquée la possibilité d'effectuer une démarche conjointe auprès du Comité Européen à la Protection des Données concernant les contrôles distants effectués par une Autorité européenne auprès d'une entité soumise au RGPD en vertu de l'article 3, mais sise dans un état tiers.

Cette réunion a également été l'occasion d'échanger avec des Agents d'Autorités de Protection des Données situées en Union européenne de récentes décisions d'adéquations prises par la Commission européenne, et plus particulièrement des catégories de données bénéficiant d'une protection particulière en application de ces décisions.

Enfin la version définitive des Lignes Directrices sur la portée extra territoriale du RGPD, qui avaient donné lieu à un document conjoint de la Suisse et de Monaco lors de leur mise en consultation publique, ont été évoquées afin d'essayer de lever les incertitudes qui subsistent.

Participation virtuelle à la 40ème réunion plénière du Comité de la Convention 108

Les 18, 19 et 20 novembre, un Agent du Secrétariat a assisté « *virtuellement* », aux côtés de la représentante de Monaco, à la 40è réunion plénière du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108) organisée exceptionnellement par visioconférence.

Plus de 150 participants issus de toutes les régions du monde se sont ainsi connectés afin d'échanger sur des sujets aussi sensibles que la reconnaissance faciale, le profilage et la cybercriminalité.

Plusieurs rapports dont ceux de Monsieur Pat Walsche sur les « Identités numériques » et de Monsieur Colin Bennett sur « *Le traitement des données à caractère personnel par et pour les*

campagnes politiques » ont donné lieu à des échanges de vues avec les experts et les délégations ont été invitées à faire part de leurs commentaires avant la fin de l'année 2020, pour finalisation desdits rapports.

Enfin, des Lignes directrices sur « *La protection des données personnelles des enfants dans un cadre éducatif* » ont été finalisées et adoptées.

Finalisation d'une recommandation dans le cadre du Groupe de Berlin

Si cette année aucune réunion de l'« *International Working Group on Data Protection in Telecommunications* », n'a pu se tenir en présentiel, deux agents de la CCIN ont tout de même participé à la rédaction d'une recommandation sur le suivi et le ciblage dans la publicité en ligne.

Soumise exceptionnellement à une procédure de vote écrit, cette recommandation qui a été adoptée à l'unanimité par les membres du groupe, a pour objet d'accompagner les législateurs, les autorités de protection des données et les responsables de traitement pour faire face aux nombreux problèmes liés au fort développement du marché numérique.

Ces problèmes sont essentiellement les suivants :

un manque de transparence et de lisibilité : la plupart des utilisateurs ignorent non seulement que les exploitants de sites internet et les fournisseurs d'applications installent des dispositifs de suivi sur leurs terminaux et appareils mais également que les technologies intégrées permettent à des tiers d'installer des cookies de traçage, de collecter les empreintes digitales, de télécharger du contenu par le biais des pixels, etc ;

un manque de contrôle : pratiquement tous ces services internet contiennent des outils de suivi qui vont bien au-delà de ce qui est nécessaire et, souvent, les utilisateurs ne disposent pas de possibilités effectives pour stopper cette collecte de données lorsqu'ils souhaitent accéder à des pages internet/ou applications ;

une absence de minimisation des données : cet ecosystème numérique dans son ensemble est en effet basé sur la collecte d'un maximum de données, aussi détaillées et personnalisées que possible ;

une érosion de la protection des données sensibles : les pratiques d'exploitation des données dans cet ecosytème peuvent aussi concerner des catégories spéciales de données ou des données sensibles, telles que par exemple, les données de santé, des données concernant la vie sexuelle d'un individu ou son orientation sexuelle ou encore des données révélant des opinions politiques ;

un profilage des individus puisque la décision du contenu ou de la publicité qui sera présenté(e) à une personne ciblée individuellement est le résultat des données collectées et agrégées sur ladite personne ;

un manque de licéité : les différents acteurs de la publicité numérique semblent s'appuyer sur une variété de bases légales pour leurs traitements de données personnelles. Il n'est toutefois souvent pas évident de déterminer quelle base juridique a été utilisée pour le traitement de données et donc de vérifier si les dispositions légales ont été respectées.

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.

11

FICHES PRATIQUES

TELETRAVAIL ET PROTECTION DES DONNEES PERSONNELLES

Le 5 mai 2020, le Conseil National a adopté le projet de Loi n°1.014, qui favorise entre autres le recours au télétravail.

Ce vote a donné lieu à la publication en date du 15 mai 2020 de la Loi n° 1.488 du 11 mai 2020 interdisant les licenciements abusifs, rendant le télétravail obligatoire sur les postes le permettant et portant d'autres mesures pour faire face à l'épidémie de COVID-19.

Toutefois si l'intitulé de cette Loi mentionne que le télétravail est rendu obligatoire, les articles 10 et 11 de ce texte soumettent la mise en place du télétravail à deux conditions cumulatives :

- l'accord du salarié,
- la mise à disposition par l'employeur des moyens techniques et matériels nécessaires à un tel exercice.

Aussi, face à la généralisation récente du télé-travail, en Principauté, la CCIN a jugé nécessaire de rappeler les bonnes pratiques à adopter tant côté employeurs que côté salariés afin d'assurer la sécurité des systèmes d'information, la protection des données personnelles et le respect de la vie privée des salariés.

Travailler depuis son domicile n'est en effet souvent pas aussi sécurisé qu'au sein de son entreprise, ce qui est une aubaine pour les pirates informatiques, toujours prêts à profiter de la moindre faille de sécurité.

Le travail à distance effectué le plus souvent de son domicile ne doit pas conduire à une surveillance constante et inopportune du travail ou du temps de travail des salariés, ni à enfreindre le nécessaire respect de leur vie privée et de celle de leur entourage.

Recommandations pour les employeurs

Il est important de prendre à la fois des mesures pour assurer l'information et la sensibilisation des salariés et des mesures techniques pour sécu-riser le système d'information.

Les mesures pour assurer l'information et la sensibilisation des employés

Sensibilisez vos employés. Quelles que soient les solutions technologiques adoptées, vous devez sensibiliser dès le départ vos employés aux enjeux de sécurité liés au télétravail en les formant aux meilleurs usages et en leur faisant prendre conscience des risques que leurs actions (ou manque d'actions) peuvent avoir sur la sécurité du système d'information (par exemple l'absence de mise à jour d'un antivirus ou l'utilisation d'un Wifi non sécurisé).

Encadrez les usages, par exemple par le biais d'une charte informatique ou de tout autre docu-ment détaillant de manière claire les bonnes pratiques à adopter, les restrictions apportées et les procédures à respecter.

Apportez un soutien réactif à vos employés en télétravail en donnant au service technique (ou tout autre service dédié) les moyens de répondre rapidement et efficacement aux questions posées et/ou aux problèmes techniques rencontrés par lesdits employés. Cela permettra d'éviter que ceux-ci n'essaient de résoudre les problèmes par eux-mêmes, souvent au détriment de la sécurité informatique de la société.

Les mesures techniques pour sécuriser le système d'information

Catégorisez les données et analysez les risques pour une plus grande sécurité informatique. Pour cela, il convient d'identifier clairement les risques que votre société peut encourir, en classant notamment les données selon leur sensibilité afin d'envisager pour certaines d'entre elles d'en interdire l'accès à distance, ou pour d'autres de mettre en place des mécanismes de sécurité renforcés.

Vous devez fournir à vos employés les équipe-ments nécessaires (PC, téléphone, tablette...) à leur travail. Ces équipements seront ainsi sécurisés et maîtrisés par l'entreprise.

Mettez en place un système d'authentification à double niveau afin de limiter les risques d'intrusion. Il est en effet indispensable d'identifier avec certitude chaque employé. Aussi, lorsqu'un employé se connecte au réseau de l'entreprise, il convient de lui demander, par exemple, de renseigner au préalable un identifiant et mot de passe, puis un code à usage unique généré par une application ou un « porte-clef ».

Equipez tous les postes de travail des employés au minimum d'un pare-feu, d'un antivirus et d'un outil de blocage de l'accès aux sites malveillants. Les solutions antivirales utilisées doivent être des versions professionnelles afin de protéger l'entreprise de la plupart des attaques virales connues. Par ailleurs, les mises à jour de sécurité doivent être déployées dès qu'elles sont disponibles, les cybercriminels mettant peu de temps à exploiter les failles lorsqu'ils en ont connaissance.

Sécurisez vos accès extérieurs en mettant en place un VPN (Virtual Private Network ou « *réseau privé virtuel* ») pour éviter l'exposition directe de vos accès sur internet. Optez pour l'authentification du VPN, de préférence à deux facteurs pour vous prémunir de toute usurpation. Outre le chiffrement de vos connexions extérieures, ce dispositif permet également de renforcer la sécurité de vos accès distants en les limitant aux seuls équipements et seules personnes authentifiés.

Renforcez votre politique de gestion des mots de passe des utilisateurs en télétravail, mais aussi de ceux en charge du support informatique, en vous assurant que lesdits mots de passe sont suffisamment longs, complexes et uniques (combinaison de majuscules, minuscules, chiffres et caractères spéciaux) sur chaque équipement ou service utilisé. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible.

Utilisez des protocoles garantissant la confidentialité et l'authentification du serveur destinataire en vous assurant que vous disposez bien des versions les plus récentes de ces protocoles.

Mettez en place une journalisation systématique de l'activité de tous vos équipements d'infrastructure (serveurs, pare-feu, proxy…) et consultez régulièrement les journaux d'accès aux services accessibles à distance pour détecter tout comportement suspect. Prévoyez également une durée de rétention suffisamment longue de tous les accès et activités de vos équipements d'infrastructure, voire des postes de travail. Cette journalisation et cette consultation des accès vous permettront de détecter toute activité anormale qui pourrait être le signe d'une cyberattaque, tels une connexion suspecte d'un utilisateur inconnu, ou d'un utilisateur connu en dehors de ses horaires habituels, ou encore un volume inhabituel de téléchargement d'informations. Elles vous permettront également de comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier.

Mais attention: si cette vérification des accès et de l'activité sur vos équipements conduit à la surveillance du travail ou du temps de travail de vos employés l'article 11-1 de la Loi n° 1.165 relative à la protection des informations nominatives s'applique et ces mesures de surveillance sont soumises à l'autorisation préalable de la CCIN.

De plus vos salariés doivent être préalablement informés de l'existence de telles mesures de surveillance de leur activité.

Nous vous invitons à vous reporter à la recommandation de la CCIN sur la gestion des habilitations et des accès informatiques disponible sur notre site internet.

Ne rendez pas directement accessibles les interfaces de serveurs non sécurisées. De manière générale, limitez le nombre de services mis à disposition au strict minimum pour réduire les risques d'attaques.

Durcissez les sauvegardes de vos données et activités. Celles-ci doivent être réalisées et testées régulièrement pour s'assurer qu'elles fonctionnent. De même, il est important de vous assurer du niveau de sauvegarde de vos hébergements externes (cloud, site Internet d'entreprise, service de messagerie...) pour vous assurer que le service souscrit est bien en adéquation avec les risques encourus par l'entreprise.

Mettez en place des dispositifs de mise en veille automatique. Les équipements fournis à vos salariés doivent se mettre en veille automatiquement après un bref laps de temps sans activité, et ce afin d'éviter que toute personne non autorisée puisse accéder aux informations accessibles depuis votre système d'information.

Si vous avez fourni des « webcams » à vos salariés : afin de préserver la vie privée des salariés et de leur entourage les caméras ne doivent pas être activées de manière permanente, mais uniquement pour des circonstances spécifiques (participation à certaines réunions de travail par visioconférence par exemple). Cependant vos salariés doivent pourvoir refuser d'utiliser la caméra, sauf justification étayée le nécessitant. Dans le cas contraire le recours à la conférence téléphonique constitue une modalité adéquate de participation aux réunions de travail.

Les visioconférences ou les conférences téléphoniques ne doivent pas donner lieu à enregistrements, sauf justification particulière à des fins probatoires par exemple. Si tel est le cas les participants doivent en être préalablement informés.

Recommandations pour les employés

Suivez scrupuleusement les consignes de votre employeur en matière de sécurité, en respectant notamment la charte de l'entreprise si un tel document a effectivement été mis en place. En cas de difficultés à appliquer les mesures prescrites, il convient d'en informer immédiatement l'entreprise qui seule sera en mesure d'y remédier. .

Communiquez en toute sécurité en privilégiant les canaux de communication interne de votre entreprise.

Sécurisez votre connexion internet. Le Wi-Fi peut être un point d'accès très fragile à votre ordinateur pour les hackers. Or, beaucoup de gens ont installé leur box Internet sans nécessairement changer les mots de passe par défaut ou bloquer certains accès. Vous devez donc vous assurer que vous avez bien activé les protections de votre box internet notamment en matière de Wi-Fi (chiffrement WPA2 ou WPA3) et de pare-feu intégré. Pensez également à mettre à jour régulièrement ladite box soit en la redémarrant, soit depuis son interface d'administration.

Ne faites pas chez vous ce que vous ne feriez pas au travail. Cela implique notamment de ne pas vous rendre sur des sites suspects et de n'installer des applications sur vos équipements professionnels qu'après l'accord du service informatique de votre entreprise. Par ailleurs, il convient de limiter au maximum les usages récréatifs (réseaux sociaux par exemple) sur vos équipements professionnels.

Renforcez vos mots de passe. La majorité des attaques informatiques étant due à des mots de passe trop simples, il est important d'utiliser des mots de passe suffisamment longs, complexes et différents, en mélangeant majuscules, minuscules, chiffres et caractères spéciaux, sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible.

Séparez votre usage professionnel de votre usage personnel. L'activité professionnelle doit se faire sur vos moyens professionnels et seulement sur vos moyens professionnels et l'activité personnelle doit se faire uniquement sur vos équipements personnels. Il convient ainsi de créer des comptes différents sur les sites ou les logiciels que vous utilisez. De même, le VPN fourni par l'entreprise doit être utilisé uniquement pour télétravailler et non pour surfer sur les sites de streaming vidéo !

Appliquez les mises à jour de sécurité sur tous vos équipements connectés (PC, tablettes, téléphones...) dès qu'elles vous sont proposées afin de corriger les failles de sécurité qui pourraient être utilisées par des pirates pour s'y introduire et les utiliser pour attaquer le réseau de votre entreprise au travers de vos accès.

Méfiez-vous des messages (email, SMS,...) comprenant une demande douteuse ou un contenu inattendu. Il peut en effet s'agir d'une attaque par hameçonnage destinée à vous dérober des informations confidentielles (identifiant, mots de passe), de l'envoi d'un virus par pièce-jointe ou d'un lien qui vous attirerait sur un site piégé, ou encore d'une tentative d'arnaque aux faux ordres de virement. Ne cliquez jamais sur les pièces jointes/liens dans les messages, demandez toujours confirmation à l'émetteur par un autre moyen, et en cas de doute, contactez le service informatique de votre société.

Sauvegardez régulièrement votre travail, si possible sur le réseau de l'entreprise, ou par le biais des moyens qu'elle met à disposition à cet effet (support externe chiffré que vous débranchez une fois la sauvegarde effectuée.)

Utilisez les équipements et outils fournis par votre entreprise (ordinateur, téléphone, VPN...) pour le télétravail.

BONNES PRATIQUES EN MATIERE DE SITES INTERNET

Le site internet est désormais un outil incontournable de la vie économique. Les entreprises, les commerçants, les entrepreneurs individuels, les personnes exerçant une activité libérale et même les personnes privées mettent en place leur site internet afin de se faire connaître, informer, présenter leurs services et produits ou encore proposer une vente à distance.

Le site internet joue également un rôle important pour attirer des clients et entretenir une relation avec eux.

Aussi, que le site internet soit un simple « *site vitrine* » ou bien un « *site marchand* », il implique dans l'immense majorité des cas une collecte de données personnelles par le biais d'une rubrique contact, d'un formulaire en ligne, de la création d'un compte client ou encore de la mise en place de cookies de navigation.

La vocation de cette fiche pratique est donc d'aider les responsables de traitement à adopter les bonnes pratiques pour assurer la confidentialité et la sécurité de ces données.

SITE VITRINE

Un « ***site vitrine*** » sert à présenter une entreprise, une administration, une association (...), son activité, ses services et/ou ses produits.

Il peut également proposer d'autres fonctionnalités comme par exemple :

- un formulaire de contact ;
- un abonnement à une lettre d'informations (Newsletter).

SITE MARCHAND

Un « ***site marchand*** » ou « ***site de vente en ligne*** » sert principalement à proposer des services et/ou des produits à la vente.

Une autre alternative peut également être un « ***site marketplace*** » dont la fonction principale est l'intermédiation de vente à distance par la vente de produits de commerçants ainsi que leur présentation. L'internaute peut ainsi effectuer ses achats chez divers commerçants sur un même site internet avec un seul compte client.

Un devoir d'information sur la collecte de données personnelles

Les personnes concernées doivent être informées, dans les conditions générales et/ou dans une rubrique dédiée à la politique de confidentialité des données personnelles sur le site, de leurs droits en application de l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

- Sur les personnes concernées

En vertu de l'article 1er de la Loi n° 1.165 qui dispose que « *La personne concernée par un traitement d'informations nominatives est celle à laquelle se rapportent les informations qui font l'objet du traitement* », les données suivantes des internautes sont le plus souvent collectées par les sites internet :

« ***Tous les visiteurs du site*** » : notamment en cas de présence de cookies, de sites de vente en ligne ;

« ***les salariés*** » : lorsque leurs informations nominatives sont affichées sur le site ou font l'objet d'une traçabilité (par exemple : nom, prénom, fonction, contact, photo, login, logs de connexion) ;

« ***les clients*** » : notamment en cas de création de comptes.

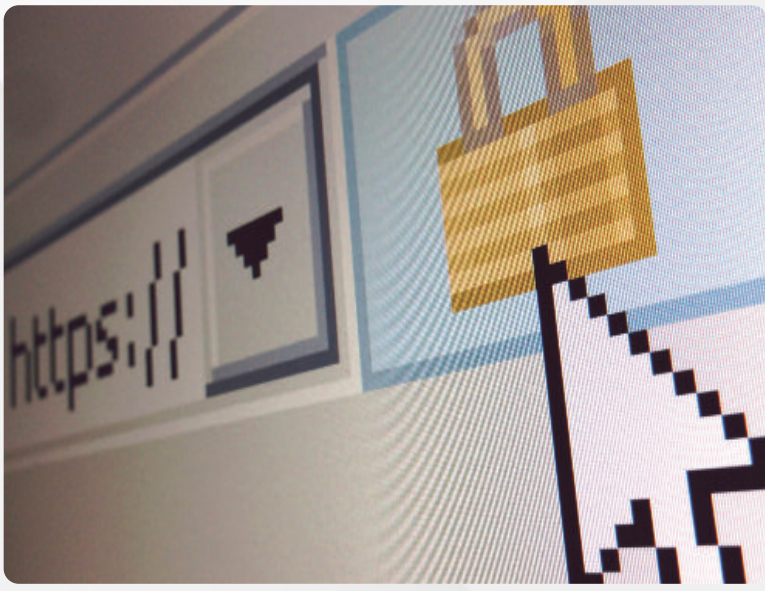
- Sur les mentions d'information à fournir

En vertu de l''article 14 de la Loi 1.165, « *Les personnes auprès de qui des informations nominatives sont recueillies doivent être averties :*

- *de l'identité du responsable du traitement et le cas échéant de celle de son représentant à Monaco ;*
- *de la finalité du traitement ;*
- *du caractère obligatoire ou facultatif des réponses ;*
- *des conséquences à leur égard d'un défaut de réponse ;*
- *de l'identité des destinataires ou des catégories de destinataires ;*
- *de leurs droits d'opposition, d'accès et de rectification relativement aux informations les concernant ;*
- *de leur droit de s'opposer à l'utilisation pour le compte de tiers, ou à la communication à des tiers d'informations nominatives les concernant à des fins de prospection, notamment commerciale* ».

Pour les sites internet, cette information doit se faire par le biais des **Conditions Générales** et/ou d'une **page consacrée à la politique de confidentialité des données** personnelles accessible facilement sur le site internet.

Il existe toutefois plusieurs situations dans lesquelles l'information ne suffit pas. Il faut ainsi expressément demander l'accord de l'internaute dans le cadre de la prospection commerciale par courrier électronique et dans certains cas, lors de l'utilisation de cookies.



Les cookies sont de petits fichiers qui sont insérés sur l'ordinateur d'un internaute par le site web au moment de sa consultation. Ces fichiers enregistrent ensuite des informations concernant l'internaute, il peut s'agir d'informations nominatives le concernant. Les informations ainsi collectées peuvent ensuite être analysées afin de faciliter la navigation sur le site, proposer des publicités ciblées et analyser les habitudes de navigation.

Néanmoins, les cookies n'ont pas accès au contenu de l'ordinateur de l'internaute.

Il existe plusieurs types de cookies :

- **les cookies techniques/fonctionnels (dont cookies de mesure d'audience) ;**
- **les cookies d'applications tierces ;**
- **les cookies de partenaires publicitaires ;**
- **les cookies optionnels.**

Lorsque le consentement est nécessaire, il convient de prévoir une possibilité simple et rapide d'annulation de celui-ci.

- Cas des transferts de données vers un pays ne disposant pas d'un niveau de protection adéquat

Un tel transfert des données collectées par les sites internet, notamment vers les Etats-Unis d'Amérique, peut survenir notamment lorsque lesdits sites utilisent des prestataires pour les services suivants :

- **Statistiques, cookies, Google Analytics ;**
- **Newsletter ;**
- **Hébergement ;**
- **ReCaptcha ;**
- **Paiement en ligne.**

NB : La liste des pays disposant d'un niveau de protection adéquat est disponible sur le site Internet de la CCIN.

L'internaute devra alors être averti de ce transfert, le plus souvent y consentir, et des mesures devront impérativement être prises pour assurer la confidentialité et la sécurité des données transférées.

Google Analytics

Lorsqu'un site internet utilise Google Analytics, les données suivantes sont envoyées à Google Inc, aux Etats-Unis : adresse IP, nom de domaine internet de l'internaute, pages visitées et leur nombre, nombre d'affichage par page, durée passée sur chaque page, nombre de clics, nom et version du navigateur web de l'internaute, système d'exploitation de l'internaute, horodatage d'accès au site et des pages visitées sur le site.

La Commission a les exigences suivantes :

- qu'un bandeau « *Cookies* » soit impérativement mis en place afin de permettre à l'internaute d'accepter ou de refuser le dépôt des cookies sur son terminal ;
- ce bandeau d'information doit impérativement apparaître à l'ouverture du site avant dépôt de tout cookie et sans que l'internaute n'ait à effectuer une quelconque démarche ;
- ce bandeau doit informer les internautes du transfert de leurs données vers les Etats-Unis, pays ne disposant pas d'un niveau de protection adéquat ;
- en cas de refus de dépôt de cookies, l'internaute doit être informé que sa demande a effectivement été prise en compte. Il doit également pouvoir poursuivre sa navigation ;
- l'internaute, dans la rubrique dédiée à la politique cookie, doit pouvoir changer ses paramètres et revenir ainsi à tout moment sur son consentement.

Il existe toutefois des alternatives européennes (Union européenne) à Google Analytics. Leur utilisation ne nécessite pas la mise en place d'un **bandeau** relatif aux cookies sur le site internet car il n'y a pas de transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat.

Par ailleurs, si les deux derniers octets de l'adresse IP sont anonymisés, il n'y a pas lieu non plus d'obtenir le consentement de l'internaute pour la collecte de données statistiques.

Mailchimp est une plateforme de marketing automation et un service de marketing par courriel. Elle propose à ses clients de créer des campagnes de communication par courriel. L'utilisateur a la possibilité de personnaliser ses campagnes en fonction de critères de segmentation de sa base de contacts. La plate-forme propose également l'envoi de courriels automatiques en fonction d'événements ou de caractéristiques associées à un contact.

Ladite plateforme est située aux Etats-Unis et implique donc un transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat dès lors qu'un site internet l'utilise.

La Commission demande en conséquence que toute personne souhaitant s'abonner à une lettre d'information gérée par cette plateforme soit avertie par un message que ses données seront hébergées par le prestataire Mailchimp basé aux Etats-Unis.

Elle demande également que cette personne puisse se désinscrire à tout moment de la lettre d'information et revenir ainsi sur son consentement.

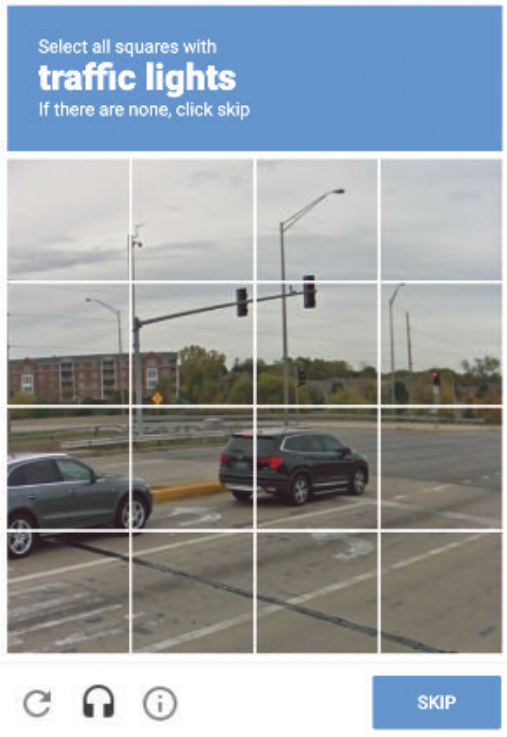
ReCaptcha Google

La fonctionnalité « *ReCaptcha* » distingue les humains des robots. Elle correspond à une case « *je ne suis pas un robot* » à cocher, très souvent complétée par un test de reconnaissance d'images.

La Commission interdit l'utilisation de ce ReCaptcha Google qui entraîne un transfert des informations nominatives vers les Etats-Unis si le consentement des utilisateurs n'est pas au préalable recueilli.

Pour distinguer un humain d'un robot, des solutions proposées par des pays disposant d'un niveau de protection adéquat et similaires à ce ReCaptcha, sont toutefois disponibles sur le marché.

Une fonctionnalité de ReCaptcha peut également être développée en interne par les départements techniques des responsables de traitement.



Une maîtrise des données personnelles collectées

Tous les sites internet ne collectent pas le même nombre de données ni les mêmes catégories. Cela dépend des fonctionnalités des sites créés.

Une fois ces fonctionnalités identifiées, il appartiendra au responsable de traitement de déterminer quelles données sont réellement nécessaires pour chacune de ces fonctionnalités et d'appliquer des durées de conservation adaptées à chacune des catégories de données ainsi collectées.

Sur les fonctionnalités des sites internet

Le tableau ci-dessous présente les fonctionnalités les plus souvent rencontrées

SITE VITRINE

- Présenter l'entreprise, l'association (...) ;
- Trombinoscope ;
- Transmettre les informations aux prospects et aux clients sur la société et/ou sur les produits, aux visiteurs sur l'association, ... ;
- Diffuser les actualités de l'entreprise, l'association (...) ;
- Communiquer les coordonnées ;
- Mettre à disposition un formulaire de contact ;
- Inscription à une Newsletter ;
- Communiquer les liens vers les réseaux sociaux ;
- Protection ReCaptcha ;
- Communiquer les liens hypertextes ou les références à d'autres sites internet ;
- Produire des statistiques d'audience et analyser le trafic web (par exemple par le biais de Google Analytics -cookies).

Attention : Si un site comporte des espaces de discussion, les sujets qui y seront abordés devront être maîtrisés afin d'éviter toute mise en cause de la responsabilité fondée sur des propos tenus par des utilisateurs (pédophilie, incitation à la violence, à la haine raciale, etc.). Cela passera par la désignation d'un modérateur.

SITE MARCHAND

- Présenter l'entreprise ;
- Trombinoscope ;
- Transmettre les informations aux prospects et aux clients sur la société et/ou sur les produits ;
- Diffuser les actualités de l'entreprise ;
- Communiquer les coordonnées de l'entreprise ;
- Mettre à disposition un formulaire de contact ;
- Inscription à une Newsletter ;
- Communiquer les liens vers les réseaux sociaux ;
- Protection ReCaptcha ;
- Communiquer les liens hypertextes ou les références à d'autres sites internet ;
- Produire des statistiques d'audience et analyser le trafic web (par exemple par le biais de Google Analytics -cookies) ;
- Vente à distance (achat en ligne, traiter les commandes, réaliser les livraisons, historique des achats, etc.) ;
- Création et/ou gestion d'un compte client ;
- Mise à disposition d'un panier pour les achats en ligne ;
- Paiement en ligne ;
- Etablissement de factures ;
- Permettre de transmettre à la société des réclamations et gestion du SAV ;
- Suivi de la relation client (réalisation d'actions de fidélisation, de prospection, de sondage, de test produit et de promotion).

Sur les données collectées

L'article 10.1 de la Loi 1.165 demande que les informations traitées soient : « ***adéquates, pertinentes et non excessives*** *au regard de la finalité pour laquelle elles sont collectées et pour laquelle elles sont traitées ultérieurement (...).* »

Le responsable de traitement doit donc faire attention à ne collecter que les seules informations dont il a besoin pour chacune des fonctionnalités de son site internet. Si celui-ci est déjà en place, il convient de passer en revue les données collectées et de supprimer celles qui ne sont pas ou plus nécessaires.

Cela peut se traduire par exemple par un ajustement des formulaires permettant de collecter les données personnelles des internautes.

Ci-dessous les catégories de données les plus souvent collectées :

SITE VITRINE

Catégorie « *Identité* » :

- Salariés : nom, prénom, photo ;
- Personnes tierces : nom, prénom, photo des événements (si oui, le consentement a-t-il été obtenu ?).

Catégorie « *Rubrique Contact* » :

- nom, prénom, adresse email, raison sociale, contenu du message.

Catégorie « *Données d'identification électronique* » :

- logs de connexion des administrateurs, des prestataires et éventuellement des clients.

Catégorie « Cookies de Google Analytics » :

- adresse IP, nom du domaine internet de l'internaute, pages visitées et leur nombre, nombre d'affichages par page, durée passée sur chaque page, nombre de clics, nom et version du navigateur web de l'internaute, système d'exploitation de l'internaute, horodatage d'accès au site et des pages visitées sur le site.

SITE DE VENTE EN LIGNE

Catégorie « *Identité* » :

- Salariés : nom, prénom, photo ;
- Personnes tierces : nom, prénom, photo des événements (si oui, le consentement a-t-il été obtenu ?).

Catégorie « *Rubrique Contact* » :

- nom, prénom, adresse email, raison sociale, contenu du message.

Catégorie « *Données d'identification électronique* » :

- logs de connexion des administrateurs, des prestataires et éventuellement des clients.

Catégorie « *Cookies de Google Analytics* » :

- adresse IP, nom du domaine internet de l'internaute, pages visitées et leur nombre, nombre d'affichages par page, durée passée sur chaque page, nombre de clics, nom et version du navigateur web de l'internaute, système d'exploitation de l'internaute, horodatage d'accès au site et des pages visitées sur le site ;

Catégorie « *Informations temporelles, horodatage* » :

- Horodatage des transactions, commandes, échanges de service clients et autres communications avec les clients, fournisseurs et sous-traitant.

Catégorie « *Vente en ligne/informations bancaires* » :

- nom, prénom, numéro de carte bancaire.

Catégorie « *Panier* » :

- nom, prénom, adresse, détails des achats.

Sur la durée de conservation des données collectées

L'article 10.1 de la Loi 1.165 précise que les informations traitées doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant* « ***une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées*** *ou pour laquelle elles sont traitées ultérieurement* ».

Ainsi il est important de respecter les règles suivantes :

- supprimer les données et le contact d'un internaute qui ne donne pas de réponse aux sollicitations du responsable de traitement durant un délai de 3 ans maximum ;
- conserver les données relatives à la navigation d'un internaute pendant 13 mois seulement, à compter de la date de dépôt du cookie ;
- supprimer les données non-nécessaires à la réalisation d'un objectif interne, une fois celui-ci atteint ;
- supprimer systématiquement les données des personnes ayant demandé à ne plus être sollicitées par le responsable de traitement, ou les archiver selon les cas à des fins de paiement ou de prescription si des transactions ont eu lieu.

A titre d'exemple, le tableau ci-dessous récapitule les durées recommandées par la Commission pour les catégories de données les plus communément rencontrées :

SITE VITRINE	SITE DE VENTE EN LIGNE
Catégorie « *Identité* » : • Salariés : tant que la personne est en poste ; • Personnes tierces : selon le consentement/tant que le site est en place /politique d'archivage/autres. **Catégorie « *Rubrique Contact* » :** • Le temps de traitement de la demande.	**Catégorie « *Identité* » :** • Salariés : tant que la personne est en poste ; • Personnes tierces : selon le consentement/tant que le site est en place /politique d'archivage/autres. **Catégorie « *Rubrique Contact* » :** • Le temps de traitement de la demande.

SITE VITRINE

Catégorie « *Identité* » :

- Salariés : tant que la personne est en poste ;
- Personnes tierces : selon le consentement/tant que le site est en place /politique d'archivage/autres.

Catégorie « *Rubrique Contact* » :

- Le temps de traitement de la demande.

Catégorie « Données d'identification électronique » :

- 1 an maximum à compter de la collecte.

Catégorie « *Cookies de Google Analytics* » :

- 13 mois maximum conformément à la délibération n° 2019-083 du 15 mai 2019 portant recommandation sur les modalités de dépôt et la durée de conservation des cookies et autres traceurs sur les terminaux d'utilisateurs de réseaux de communication électronique (NB : cette durée maximum vaut de manière générale pour tous les cookies).

Catégorie « Newsletter » :

- Tant que la personne est inscrite.

SITE DE VENTE EN LIGNE

Catégorie « *Identité* » :

- Salariés : tant que la personne est en poste ;
- Personnes tierces : selon le consentement/tant que le site est en place /politique d'archivage/autres.

Catégorie « *Rubrique Contact* » :

- Le temps de traitement de la demande.

Catégorie « *Données d'identification électronique* » :

- 1 an maximum à compter de la collecte.

Catégorie « *Cookies de Google Analytics* » :

- 13 mois maximum conformément à la délibération n° 2019-083 du 15 mai 2019 portant recommandation sur les modalités de dépôt et la durée de conservation des cookies et autres traceurs sur les terminaux d'utilisateurs de réseaux de communication électronique (NB : cette durée maximum vaut de manière générale pour tous les cookies).

Catégorie « *Newsletter* » :

- Tant que la personne est inscrite.

Catégorie « *Informations temporelles, horodatage* » :

- Jusqu'à effacement du compte client sur demande du client et expiration du droit de garantie sur les produits ou services achetés.

Catégorie « *Vente en ligne/informations bancaires* » :

- Attention en cas de collecte de cartes bancaires. Les données relatives aux cartes bancaires doivent en effet être supprimées une fois la transaction réalisée. Les factures peuvent en revanche être conservées 10 ans.

Catégorie « *Panier* » :

- Si la personne ne passe pas commande, les données ne doivent pas être conservées au-delà de 10 jours.

Cas particulier de la conservation des données bancaires

Les données bancaires peuvent être conservées pour une finalité de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires, treize mois suivant la date de débit. Ce délai peut être étendu à quinze mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé.

Ces données peuvent être conservées plus longtemps sous réserve d'obtenir le **consentement exprès** du client, préalablement informé de l'objectif poursuivi (faciliter le paiement des clients réguliers, par exemple). Ce consentement peut être recueilli par l'intermédiaire d'une case à cocher, et non **précochée par défaut**, et ne peut résulter de l'acceptation de conditions générales.

Les données relatives au cryptogramme visuel ne doivent pas être stockées.

Lorsque la date d'expiration de la carte bancaire est atteinte, les données relatives à celle-ci doivent être supprimées.

Cas particulier de la conservation des copies des documents d'identité

Les copies des documents d'identité pourront être conservées au maximum 6 mois lorsqu'elles servent de justificatifs relatifs à la vérification de l'identité d'un titulaire de carte bancaire, et doivent être détruites dès que la vérification de l'identité de la personne concernée est effectuée s'agissant des demandes de remboursement ou de paiement à distance.

Une obligation de sécurité des données

L'article 17 de la Loi 1.165 dispose que « *Le responsable de traitement ou son représentant est tenu de prévoir des mesures techniques et* ***d'organisation appropriées pour protéger les informations nominatives*** *contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions d'informations dans un réseau, ainsi que contre toute autre forme de traitement illicite* ».

C'est ainsi qu'en matière de sites internet, il doit prendre des mesures assurant non seulement la confidentialité des données mais également leur sécurité.

Des mesures pour assurer la confidentialité des données

- l'accès aux données est réservé uniquement aux seules personnes ayant à en connaître. En fonction de leur activité, ces personnes ne pourront avoir accès qu'à certaines catégories de données (le service comptable par exemple pourra n'avoir accès qu'à l'identité et à l'adresse d'un internaute ainsi qu'aux informations liées à l'achat qu'il doit facturer sans nécessairement avoir accès aux autres informations potentiellement collectées sur le client).

- l'accès aux outils et interfaces d'administration doit être réservé aux seules personnes habilitées. Il convient en particulier de limiter l'utilisation des comptes administrateurs aux équipes en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent.
- les habilitations et les mots de passe doivent régulièrement être mis à jour afin de garantir que seules les personnes habilitées peuvent accéder aux données nécessaires à la réalisation de leurs missions.
- un mécanisme de journalisation des opérations et des accès effectués sur le traitement doit être mis en place.
- les interventions de maintenance doivent faire l'objet d'une traçabilité et le matériel remisé ne devra plus contenir d'informations nominatives. Il convient d'être particulièrement vigilant lors de changements d'équipements, notamment de disques durs, qui sont une source de fuite de données si ces supports ne sont pas correctement effacés lors de leur mise au rebut.

Cas particulier de la protection des données liées à la carte bancaire

Les données nécessaires à la réalisation d'une transaction à distance par carte de paiement sont le numéro de la carte, la date d'expiration et le cryptogramme visuel.

L'utilisation de moyens de paiements en ligne et la conservation de numéros de cartes bancaires doivent faire l'objet de mesures de traçabilité permettant de détecter a posteriori tout accès illégitime aux données et de l'imputer à la personne ayant accédé illégitimement à ces données. En effet, les données de cartes bancaires étant particulièrement sensibles, il convient de savoir quelles personnes au sein du personnel du site marchand ont pu y avoir accès.

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

Lorsque le responsable de traitement conserve les numéros de carte bancaire pour une finalité de preuve en cas d'éventuelle contestation de la transaction, ces numéros doivent faire l'objet de mesures techniques visant à prévenir toute réutilisation illégitime, ou toute ré identification des personnes concernées. Ces mesures peuvent notamment consister à stocker les numéros de carte bancaire sous forme hachée avec utilisation d'une clé secrète.

En outre, compte tenu de la sensibilité de cette donnée, le numéro de la carte de paiement ne peut être utilisé comme identifiant commercial.

Le responsable de traitement, ou son prestataire, ne doit pas demander la transmission de la photocopie ou de la copie numérique du recto et/ou du verso de la carte de paiement même si le cryptogramme visuel et une partie des numéros sont masqués.

Lorsque la collecte du numéro de la carte de paiement est effectuée par téléphone, il est nécessaire de mettre en place des mesures de sécurité telle que la traçabilité des accès aux numéros des cartes. Une solution alternative sécurisée, sans coût supplémentaire, doit être proposée aux clients qui ne souhaitent pas transmettre les données relatives à leurs cartes par ce moyen.

Cas particulier de la protection des copies des documents d'identité

S'agissant des documents d'identité la Commission est particulièrement vigilante quant aux modalités de leur collecte. L'objectif est de lutter contre le vol et l'usurpation d'identité, l'utilisation illicite des informations nominatives contenues dans ces documents et les conséquences que cela peut induire pour les victimes.

En ce qui concerne les sites marchands, la collecte n'est permise qu'aux fins de s'assurer de l'identité d'un titulaire de carte bancaire ou pour gérer les demandes de paiement ou de remboursement suite à la participation à un jeu.

La Commission demande que les modalités de collecte à distance soient protégées et notamment que les copies de documents d'identité soient déposées sur une page sécurisée. C'est pourquoi elle a adopté par délibération n° 2015-113 une recommandation sur la collecte et la conservation de la copie de documents d'identité officiels, qui est disponible sur son site Internet www.ccin.mc.

La Commission recommande également que les personnes dont les copies de documents d'identité sont collectées soient invitées à transmettre celles-ci en noir et blanc et barrées, afin d'en rendre difficiles d'éventuelles reproductions.

Des mesures pour assurer la sécurité des données

Des mesures de sécurité des locaux et des systèmes d'information doivent être mises en place afin d'empêcher que les fichiers soient déformés, endommagés ou que des tiers non autorisés y aient accès.

Le protocole TLS (en remplacement de SSL) doit être mis en œuvre sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre.

L'utilisation de TLS doit être obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.

Seuls les ports de communication strictement nécessaires au bon fonctionnement des applications installées doivent être conservés. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

Le nombre de composants mis en œuvre doit être limité et mis à jour.

Une veille technique doit être mise en place afin d'assurer que la sécurité est **toujours** à jour.

DU BON USAGE DES RESEAUX SOCIAUX

Le succès planétaire des réseaux sociaux – Facebook en premier lieu – a fait rentrer la société, toutes classes confondues, dans une nouvelle ère, celle de l'exhibitionnisme numérique. Véritables phénomènes, ces réseaux sociaux provoquent des réactions extrêmes. Soit on aime, soit on n'aime pas. Pourtant à y regarder de plus près, les réseaux sociaux offrent souvent autant d'avantages qu'ils présentent d'inconvénients.

Ainsi, l'atout principal de ces plateformes interactives est sans conteste le réseautage à la fois social (puisqu'ils permettent à leurs membres de rester en contact avec leurs amis et leur famille) que professionnel (puisque certains d'entre eux permettent de nouer des contacts utiles et de trouver du travail).

Ces sites permettent également d'envoyer et de recevoir des messages, de télécharger des photos et des vidéos, d'acquérir une notoriété publique en créant un blog ou une chaine Youtube pour faire le « *buzz* » et obtenir un certain nombre de « *vue* » et de « *like* ».

Par ailleurs, ils sont aussi un outil de promotion très efficace pour une entreprise, des services, des produits ou encore des sites.

En revanche, parmi les risques principaux, nous trouvons :

- le piratage de compte qui peut aller jusqu'à l'usurpation d'identité ;
- les cambriolages lorsqu'une personne a indiqué non seulement son adresse mais également ses dates de vacances ;
- le voyeurisme lorsque des informations purement privées, telles des photos ou des vidéos sont publiées ;
- le harcèlement en ligne comme cela peut arriver par exemple dans les écoles où des adolescents menacent leurs camarades de révéler des photos coquines ;
- le partage indu d'informations sensibles à de parfaits inconnus ;
- l'utilisation non souhaitée des données collectées à des fins publicitaires ;
- les risques de dépendance, notamment chez les plus jeunes qui ne peuvent aller se coucher sans passer par la case Tik Tok.

Or, s'il n'y a souvent pas de position intermédiaire entre les adeptes du grand déballage public et ceux qui ont choisi de faire leur l'adage « *pour vivre heureux, vivons cachés* », la solution serait peut-être tout simplement d'apprendre à apprivoiser ces réseaux sociaux qui font désormais partie de notre quotidien. Cela passe notamment par :

- la connaissance des principaux réseaux et de leurs fonctionnalités ;
- l'adoption de bons comportements ;
- le paramétrage de la sécurité et de la portée des publications.

FACEBOOK

Créé en 2004, Facebook est sans conteste le réseau social le plus connu. Il permet à ses utilisateurs de publier du contenu (images, photos, vidéos, fichiers...), d'échanger des messages et d'interagir sur les messages des autres utilisateurs.

C'est également une **base de données marketing** extraordinaire pour les entreprises car toutes les classes d'âge et catégories de population y sont réunies. De ce fait, le réseau propose aux entreprises de faire des campagnes publicitaires (**Facebook Ads**) avec des ciblages très précis en fonction de leurs centres d'intérêt, leur comportement ou encore leurs critères socio-démographiques et géographiques des internautes. De plus, Facebook offre la possibilité d'analyser toutes les retombées des publicités publiées grâce à des outils statistiques très détaillés.

TWITTER

Créée en 2006, cette plateforme de microblogging **permet aux utilisateurs d'envoyer et de lire de courts messages, appelés** « *tweets* ». Ces messages de 140 caractères maximum (la limite du nombre de caractères a été doublée à 280 signes en 2017) lui permettent d'être une source **d'information en temps réel**, ce qui correspond aux attentes des nouvelles générations. Ce réseau est notamment très utilisé par les influenceurs (dirigeants, journalistes, blogueurs, politiques...) pour transmettre de l'information rapidement. Twitter permet également de diffuser des publicités à une cible très précise en fonction de ses centres d'intérêt et de critères socio-démographiques ou géographiques et d'en analyser les résultats.

INSTAGRAM

Créé en 2010 et appartenant désormais à Facebook, Instagram est un réseau social très simple d'utilisation qui permet de partager des photos et de courtes vidéos disponibles sur plateformes mobiles. Depuis 2016, les utilisateurs peuvent également réaliser et diffuser des « *stories* » qui disparaissent au bout de 24h. Il y est très rare de mettre beaucoup de textes, quelques mots et des hashtags suffisent.

YOUTUBE

Créée en 2005 et appartenant désormais à Google, YouTube est la première plateforme d'hébergement et de partage de vidéos à grande échelle. Il permet aux utilisateurs d'envoyer, de regarder, d'évaluer, de commenter et de partager sur d'autres réseaux sociaux les vidéos.

SNAPCHAT

Créée en 2011, cette application est très prisée par les jeunes. Elle permet d'envoyer des photos et vidéos qui n'apparaissent que pendant quelques secondes. L'application permet également de créer et de diffuser des stories (suite de photos et/ou vidéos) visibles à volonté mais uniquement pendant 24h.

LINKEDIN

Créé en 2003, LinkedIn est un **réseau social professionnel** qui a pour objectif de « *connecter les professionnels du monde entier afin de rendre leur activité plus productive et plus prospère* ». Les membres du réseau partagent ainsi leur identité personnelle, communiquent avec leur réseau, échangent des informations et des points de vue professionnels, publient des articles et trouvent des opportunités commerciales et de déroulement de carrière.

Le contenu de certains de ces services peut toutefois être également visible par les simples visiteurs.

PINTEREST

Créé en 2010, Pinterest est un réseau social ayant pour but le partage de **photos de qualité** dont l'audience est presque uniquement **féminine**. Une fois qu'un membre a téléchargé et partagé les images qu'il trouve intéressantes, ces images sont transformées en « PIN » et peuvent être placées, dans n'importe quel ordre, et ce, selon différentes thématiques, laissant libre cours à l'esprit créatif des utilisateurs.

Les sujets les plus populaires sur ce réseau sont la mode, la bijouterie, l'artisanat, **les voyages, l'alimentation et les loisirs créatifs.**

TIK TOK

Créée en 2014 à Shanghai (Chine), sous le nom de Musical.ly, Tik Tok est une application particulièrement populaire auprès des jeunes. Elle permet d'enregistrer de courtes vidéos de 3 à 60 secondes, sur lesquelles les utilisateurs peuvent danser, chanter en playback, relever des défis ou encore faire des sketchs.

Comme sur Instagram, Facebook et Twitter, il est possible de « *liker* », de commenter et de partager les vidéos.

Aujourd'hui la plateforme Tik Tok est sur la bonne voie pour atteindre 1,2 milliard d'utilisateurs actifs en 2021 dans le monde.

TWITCH

Lancé en 2011 et racheté par Amazon en 2014, Twitch est LE réseau social de l'interaction par excellence.

Initialement dédiée au streaming de jeux vidéo – la diffusion en direct sur Internet par des joueurs de leurs parties –, cette plateforme permet aujourd'hui aux utilisateurs de créer des chaînes et des flux en direct autour de thèmes aussi variés que la musique, la cuisine, le fitness, la politique ou encore les cours de langue.

Grâce à un système de chat live intégré, les personnes visionnant la vidéo (appelées viewers) peuvent réagir en direct par écrit via une fenêtre de messagerie instantanée et ainsi interagir avec le streameur (le diffuseur)

CLUBHOUSE

Créé en mars 2020 et uniquement disponible sur le système d'exploitation IOS sur Iphone, Clubhouse est un réseau social 100 % audio (pas de photo, pas de post, pas de hashtag) dont l'accès n'est possible que par le parrainage d'une personne déjà membre.

Une fois inscrit, l'utilisateur peut alors créer ou rejoindre des « *rooms* » (salles) dans lesquelles se déroulent des discussions en live soit avec une personne célèbre soit au sein d'un petit groupe sur n'importe quel sujet. Il peut demander à intervenir, via un petit onglet « *Lever la main* » et ce seront les administrateurs de la salle qui décideront de le faire « *monter sur scène* ».

Les bons comportements à adopter sur les réseaux sociaux

Le principe des réseaux sociaux étant en premier lieu d'échanger avec le reste du monde, l'anonymat est donc chose quasi impossible.

En revanche, en utilisant de bons comportements, il est tout à fait possible de protéger ses données personnelles et limiter les risques de dévoiler, plus que nécessaire, des pans de sa vie privée.

Bien que chaque réseau soit différent, ils sont tous susceptibles de collecter 4 types de données :

- les informations de profil (nom, âge, profession, études, etc.) ;
- les traces de votre activité (likes, partages, commentaires, adhésion à des groupes, etc.) ;
- votre activité silencieuse (chacun de vos mouvements est enregistré même si vous êtes silencieux) ;
- la géolocalisation de votre appareil (utilisée entre autres pour générer des publicités ciblées).

Pour éviter que ces données ne soient partagées sans restriction, les réseaux sociaux ont mis en place leur propre politique de sécurité avec des réglages des paramètres de confidentialité. Apprendre à connaître et à configurer ces paramètres est donc le premier bon comportement à adopter afin d'éviter toute mauvaise surprise.

Chaque réseau s'efforce de les améliorer. Ils changent donc sans arrêt, d'où l'importance de vérifier de façon régulière s'ils correspondent toujours à ce que vous souhaitez.

A titre d'exemple, il est possible sur Facebook, de configurer chaque élément séparément. Vous pouvez ainsi créer des groupes d'amis pour déterminer qui pourra voir quoi ou bien encore autoriser ou non que votre profil apparaisse sur les moteurs de recherche tels que Google.

Sur Twitter, tous les messages sont publics par défaut. Il convient donc de faire très attention avant de tweeter. Par ailleurs, pour éviter de recevoir trop de mails de la part du réseau social, il faut configurer les notifications dans les paramètres de son compte.

Il est par ailleurs très important de séparer sur n'importe quel réseau vies personnelle et professionnelle. Avec Twitter, vous pouvez ainsi vous créer deux profils et choisir les gens que vous voulez suivre en fonction de vos intérêts. De même, si vous utilisez Facebook et le réseau professionnel en ligne LinkedIn, il convient de garder le premier pour vos relations personnelles et d'opter pour le second pour vos relations de travail.

Mais avant de voir de façon plus détaillée les règles de paramétrage pour les réseaux sociaux les plus importants, le tableau suivant récapitule les comportements de base à adopter quelle que soit la plateforme utilisée.

À NE PAS FAIRE

- Ne jamais divulguer son nom d'utilisateur ou mot de passe
- Ne pas publier sa date de naissance complète qui peut être utilisée par les publicitaires
- Ne pas indiquer ses dates de vacances (responsables de certains cambriolages)
- Ne pas indiquer en permanence où l'on se trouve
- Ne pas accepter n'importe qui comme ami
- Ne pas dire tout ni communiquer ses opinions politiques, sa religion ou son numéro de téléphone
- Ne pas commenter à tort et à travers, car ce qui est écrit sur le net reste même des années après
- Ne pas laisser parler ses amis sur vous sur tout et n'importe quoi
- Ne pas diffuser des photos embarrassantes de vous et/ou de vos amis, votre famille car une fois publiées, elles deviennent incontrôlables
- Ne pas s'abonner à des applications tierces associées à Facebook (bouton j'aime par exemple)
- Ne pas lire les conditions d'acceptation avec les nouvelles versions
- Ne pas laisser les enfants seuls sur les réseaux sociaux
- Ne pas cliquer sur tous les liens partagés, car ils peuvent être infectés
- Ne pas se connecter depuis les bornes Wifi publiques

À FAIRE

- Avoir des profils séparés « *personnels* » et « *professionnels* »
- Choisir un mot de passe sûr et unique, renouvelé régulièrement
- Avoir un mot de passe différent des autres comptes (messagerie, banque...)
- Adapter les paramètres de confidentialité à vos besoins, et ne pas laisser les conditions par défaut
- S'assurer que le correspondant est bien un ami et pas une personne se faisant passer pour lui (vérifier le compte, messagerie...)
- Supprimer régulièrement les amis inopportuns
- Se poser les bonnes questions avant de publier du contenu potentiellement dangereux
- Utiliser un logiciel antivirus
- Installer la version la plus récente de son navigateur (comme Internet Explorer, Firefox...)
- Supprimer les cookies après déconnexion du réseau *(via l'option "Effacer les données de navigation"*), pour ne pas être pisté, même déconnecté
- Préférer une connexion sécurisée (avec le préfixe "*https*")
- Activer les notifications de connexion qui informent de toutes les connexions à votre compte
- Taper régulièrement votre nom dans un moteur de recherche pour vérifier quelles informations circulent sur vous

Le paramétrage de la sécurité et de la portée des publications

Les profils sociaux étant une extension de l'identité réelle de chaque utilisateur, il est donc important d'en prendre soin en maîtrisant les paramètres, filtres et autres options de sécurité mis à disposition.

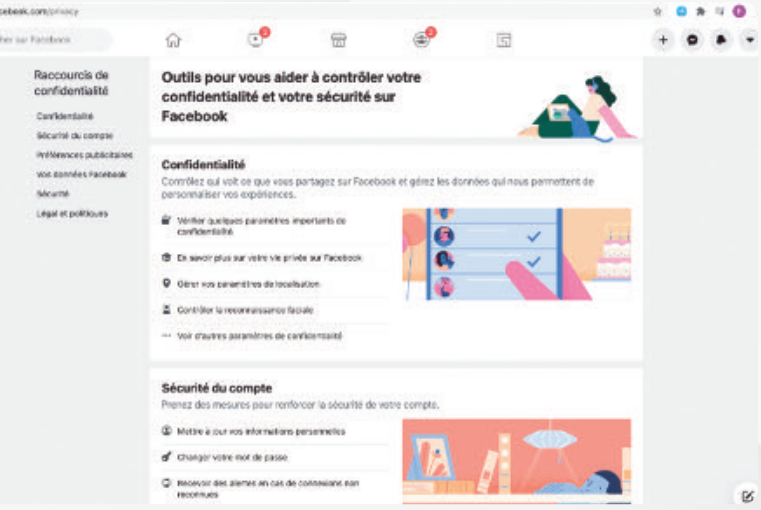
De manière générale, 3 règles de base sont à respecter ;

- une activité raisonnée ;
- une authentification forte (mot de passe unique et fort, composé de caractères minuscules, de caractères majuscules, de chiffres et de caractères spéciaux) ;
- des paramètres de sécurité et de confidentialité adaptés à vos besoins.

Les deux premières étant du seul ressort de chaque individu, nous allons maintenant passer en revue les paramètres de sécurité et de confidentialité de quelques-uns des principaux réseaux sociaux.

Les paramètres de sécurité Facebook

Réseau le plus populaire avec près de 2,8 milliards de membres, Facebook est également le réseau le plus attaqué et le plus critiqué. Pourtant, il est possible de limiter la diffusion de ses données personnelles depuis que le réseau a été forcé d'adapter sa politique de confidentialité suite à diverses actions légales menées contre lui.



Aujourd'hui, Facebook fournit des explications claires et précises dans une section intitulée **Sécurité du compte.** Par ailleurs, les paramètres de confidentialité peuvent être consultés et modifiés très facilement en cliquant sur la flèche pointant vers le bas située dans le coin supérieur droit de n'importe quelle page Facebook. Il suffit ensuite de sélectionner **Paramètres et confidentialité** dans le menu déroulant, puis de sélectionner **Raccourcis de confidentialité** dans le menu de gauche de la page qui s'est ouverte.

Parmi les paramètres à configurer, vous pourrez notamment choisir de :

Recevoir des notifications en cas de connexion depuis un autre appareil

Pour configurer cette option, il faut se rendre dans **Paramètres et confidentialité**, puis dans **Sécurité du compte** et enfin dans **Recevoir des alertes en cas de connexions non reconnues** pour choisir de recevoir des notifications. Afin d'augmenter d'un cran cette protection, il est possible de demander au réseau social d'envoyer un code de sécurité à votre portable à chaque nouvelle connexion depuis un navigateur inconnu. Pour cela, il suffit d'aller dans **Utiliser l'authentification en deux facteurs** disponible également sur la page **Sécurité du compte.**

Sur la page Sécurité et connexion, disponible dans Paramètres et confidentialité, puis dans Paramètres, un historique de vos connexions est disponible. Il indique les heures auxquelles votre compte est connecté, géolocalise la position de l'utilisateur et identifie l'appareil utilisé. Il est possible d'établir une liste des navigateurs d'où vous souhaitez pouvoir vous connecter, et d'en exclure certains.

Vous pouvez aussi choisir des contacts de confiance dans votre liste d'amis qui pourront vous aider en cas de difficultés à accéder à votre compte.

Paramétrer la confidentialité

Par défaut, un statut Facebook est public et les photos que vous publiez sont visibles de tous.

C'est donc à vous de paramétrer votre compte pour que seuls vos amis puissent voir vos photos et ce que vous publiez sur votre mur.

Pour ce faire, il faut aller dans Paramètres et confidentialité, puis dans Assistance confidentialité et enfin dans Qui peut voir ce que vous partagez pour déterminer qui a accès à vos publications, futures comme antérieures. Facebook offre la possibilité

de créer des listes d'amis afin de différencier vos « *amis proches* » - avec qui vous souhaitez partager la totalité de vos contenus vidéos, photos et partages - des « *connaissances plus éloignées* ». Il suffit pour cela de créer des listes classifiant vos « *amis* » Facebook, et de paramétrer les contenus vous concernant selon l'accès que vous leur laisserez. Néanmoins, en le faisant, vous révélez au réseau social une partie de votre vie privée et lui permettez de faire connaissance de votre cercle d'amis proches. En cas de piratage de votre compte, ces informations pourraient être exploitées.

En cas de cyberharcèlement ou d'invitations trop répétitives à jouer à une application, vous pouvez également bloquer totalement la personne importune ou l'application visée.

Sécuriser les accès à vos publications

Le réseau social propose de multiples options de sécurité qui ne sont pas activées par défaut et qui permettent par exemple de contrôler l'accès aux photos Facebook que vous postez ou aux photos taguées postées par un tiers.

Autre fonctionnalité intéressante, Facebook autorisant l'usage des pseudonymes lors de la création d'un compte, vous pouvez ne pas mentionner votre véritable nom pour garantir votre anonymat.

Facebook connait tout de vous

Souvenez-vous ! En 2007, **Max Schrems**, un étudiant en droit avait été à l'origine du plus grand recours collectif intenté en Europe contre Facebook. La croisade du jeune autrichien contre l'exploitation des données personnelles sur internet était née après qu'il ait demandé à Facebook de lui envoyer une compilation de ses informations collectées sur le réseau social. Il avait alors été choqué de recevoir un fichier de 1.222 pages répertoriant minutieusement toutes ses informations présentes sur le site, même celles qu'il pensait avoir supprimées.

Ce que Facebook sait de nous est en effet vertigineux et tout un chacun peut également s'en rendre compte très facilement. Pour récupérer votre propre dossier et savoir quelles sont les informations concrètes que Facebook possède, il suffit d'aller sur le site de Facebook, de sélectionner **Paramètres** puis de cliquer sur **Télécharger une copie de vos données Facebook**.

Il vous faudra alors simplement confirmer le mot de passe de votre compte.

Vous recevrez ensuite, dans un laps de temps variable, un e-mail avec un lien cliquable vers le téléchargement de l'archive. Après avoir cliqué sur le lien, l'ensemble de vos données sera téléchargé sur le disque dur de votre ordinateur.

Les paramètres de sécurité Twitter

« *Ce que vous dites sur les Services Twitter est visible partout dans le monde instantanément.* ***Vous êtes ce que vous tweetez !*** »

Public par défaut, ce réseau social peut inclure des photos, des vidéos et des liens vers d'autres sites (qui sont, eux aussi, publics par défaut).

La politique de confidentialité de Twitter est toutefois plutôt transparente et protectrice de votre identité visuelle. En effet, la plupart des options ne sont pas cachées, elles sont rassemblées au même endroit et leur paramétrage par défaut est souvent optimal au niveau de la sécurité. Il n'y a donc pas énormément de manipulations à faire.

Pour paramétrer votre compte il suffit d'aller sur celui-ci, de cliquer sur **Plus** dans la colonne de gauche puis de choisir **Paramètres et confidentialité** afin d'avoir accès entre autres aux pages **Sécurité et accès au compte** et **Confidentialité et sécurité.**

Parmi toutes les options proposées, vous pourrez :

- vérifier les demandes de connexion (cette fonctionnalité est désactivée par défaut) ;
- réinitialiser votre mot de passe (cette fonctionnalité est désactivée par défaut) ;
- vous connecter avec code (utile en cas d'oubli de votre mot de passe) ;
- toujours demander un mot de passe pour vous connecter à votre compte ;
- réduire aux seules personnes que vous connaissez la possibilité de vous identifier sur une photo ;
- protéger vos tweets en passant en mode protégé, ce qui vous permettra de réserver vos tweets à vos seuls abonnés. Ceux-ci disparaitront également de la recherche Google, donc vous n'aurez plus à craindre qu'on vous retrouve par ce biais ;
- désactiver la fonction détectabilité qui permet à d'autres utilisateurs de vous trouver en entrant votre numéro de téléphone ou votre adresse mail.

Les paramètres de sécurité Linkedin

Le réseau social professionnel a mis à jour ses conditions générales le 8 mai dernier afin, notamment, de permettre un meilleur contrôle des données partagées avec les annonceurs et d'encadrer les usages pour éviter le harcèlement.

Comme le précise le réseau social, le contenu partagé par ses utilisateurs peut se retrouver en dehors de ses services puisque « *Par exemple, des aperçus ou extraits de contenu peuvent être retrouvés dans des moteurs de recherche d'autres prestataires* ». Un contrôle est toutefois possible pour gérer la manière dont ces contenus sont partagés. « *Conformément aux paramètres disponibles, nous respecterons vos préférences concernant la visibilité du contenu et des informations (par exemple, le contenu des messages que vous envoyez, le partage de contenu uniquement avec des relations Linkedin, la limitation de la visibilité de votre profil pour les moteurs de recherche ou le fait de ne pas notifier votre réseau lors de la mise à jour de votre profil Linkedin). Par défaut, aucune notification n'est envoyée à vos relations ni au public pour les activités de recherche d'emploi* », peut-on ainsi lire dans l'article 2.5 des nouvelles conditions d'utilisation.

Par ailleurs, la section dédiée à la confidentialité de Linkedin, offre des informations utiles permettant aux utilisateurs de gérer leurs préférences et énumère quelques bonnes pratiques relatives à la sécurité d'un compte, parmi lesquelles :

- modifier son mot de passe régulièrement ;
- ne pas inscrire son adresse email ou son numéro de téléphone dans la section Résumé du profil ;
- activer la vérification en deux étapes ;
- signaler les contenus inappropriés ou les problèmes de sécurité.

Les paramètres de sécurité Instagram

Fin août 2017, le réseau social Instagram annonçait publiquement avoir fait l'objet d'un piratage massif des données personnelles de ses utilisateurs, concernant les numéros de téléphone et les adresses mails d'environ 6 millions de comptes, dont des célébrités.

Les hackers auraient profité d'une faille de sécurité pour mettre en vente les données en ligne, sur plusieurs sites. La faille a depuis été corrigée mais elle aura eu pour effet bénéfique de rappeler aux utilisateurs l'importance de protéger leurs informations personnelles. Vous pouvez ainsi trouver toutes les informations utiles dans les pages **Confidentialité** et **Sécurité** disponibles dans **Paramètres**, comme par exemple apprendre :

- comment contrôler votre visibilité ;
- comment résoudre les abus et bloquer les personnes ;
- comment partager les photos en toute sécurité ;
- comment signaler les comptes piratés, une usurpation d'identité...

S'il y a très peu de réglages de confidentialité, il vous est toutefois possible de sécuriser votre compte en l'activant en tant que compte privé, ce qui permet de limiter l'accès à vos photos aux seuls utilisateurs que vous avez préalablement acceptés.

Par ailleurs, il convient de noter que par défaut, Instagram épingle vos photos sur une carte visible à partir de votre profil, ce qui permet à toutes les personnes qui vous suivent de savoir exactement où vous êtes. Cette fonctionnalité peut toutefois être désactivée.

Les paramètres de sécurité Tik Tok

Conscient de l'importance de protéger les données des plus jeunes, Tik Tok a adapté les paramètres de l'application pour les utilisateurs de moins de 18 ans. Depuis janvier 2021, ceux-ci sont les suivants :

Confidentialité	Utilisateurs de moins de 16 ans	Utilisateurs entre 16 et 17 ans
Compte privé	Le compte sera réglé sur privé par défaut. Cela veut dire que seuls les utilisateurs approuvés peuvent s'abonner au compte et regarder les vidéos. La possibilité de régler son compte sur public est toutefois toujours possible.	Le compte sera public par défaut. L'utilisateur a cependant la possibilité de régler son compte sur privé. Pour cela, il faut aller dans **Moi**, appuyer sur ..., en haut à droite, puis aller dans **Confidentialité** pour activer ou désactiver **Compte privé**.
Suggérer son compte à d'autres	Ce paramètre est Désactivé par défaut. Cela signifie que le compte ne sera pas suggéré à d'autres utilisateurs. L'utilisateur a toutefois la possibilité de l'activer.	Ce paramètre est **Activé**. Pour que le compte ne soit plus suggéré à d'autres utilisateurs, il faut aller sur **Désactivé**.
Autoriser le téléchargement de ses vidéos	Ce paramètre est **Désactivé** et ne peut pas être modifié.	Ce paramètre est **Désactivé**. Pour autoriser le téléchargement de ses vidéos par d'autres utilisateurs, il faut l'activer.
Qui peut faire un Duo avec ses vidéos	Ce paramètre est défini sur **Seulement moi**. L'utilisateur est la seule personne à pouvoir faire des Duos avec ses vidéos. Ce paramètre ne peut pas être modifié.	Ce paramètre est défini sur **Amis**. Il peut être changé en **Seulement** moi ou **Tout le monde**, selon ses préférences.
Qui peut faire un Collage avec ses vidéos	Ce paramètre est défini sur **Seulement moi**. L'utilisateur est la seule personne à pouvoir faire des Collages avec ses vidéos. Ce paramètre ne peut pas être modifié.	Ce paramètre est défini sur **Amis**. Il peut être changé en **Seulement moi** ou **Tout le monde**, selon les préférences de l'utilisateur.
Qui peut commenter ses vidéos	Ce paramètre est défini sur **Amis**. Cela veut dire que seules les personnes abonnées au compte de l'utilisateur et auxquelles il est abonné peuvent commenter des vidéos. L'utilisateur peut le changer en **Personne** pour empêcher d'autres utilisateurs de commenter ses vidéos.	Ce paramètre est défini sur **Tout le monde**. Il peut cependant être modifié par l'utilisateur pour limiter qui peut commenter ses vidéos.

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