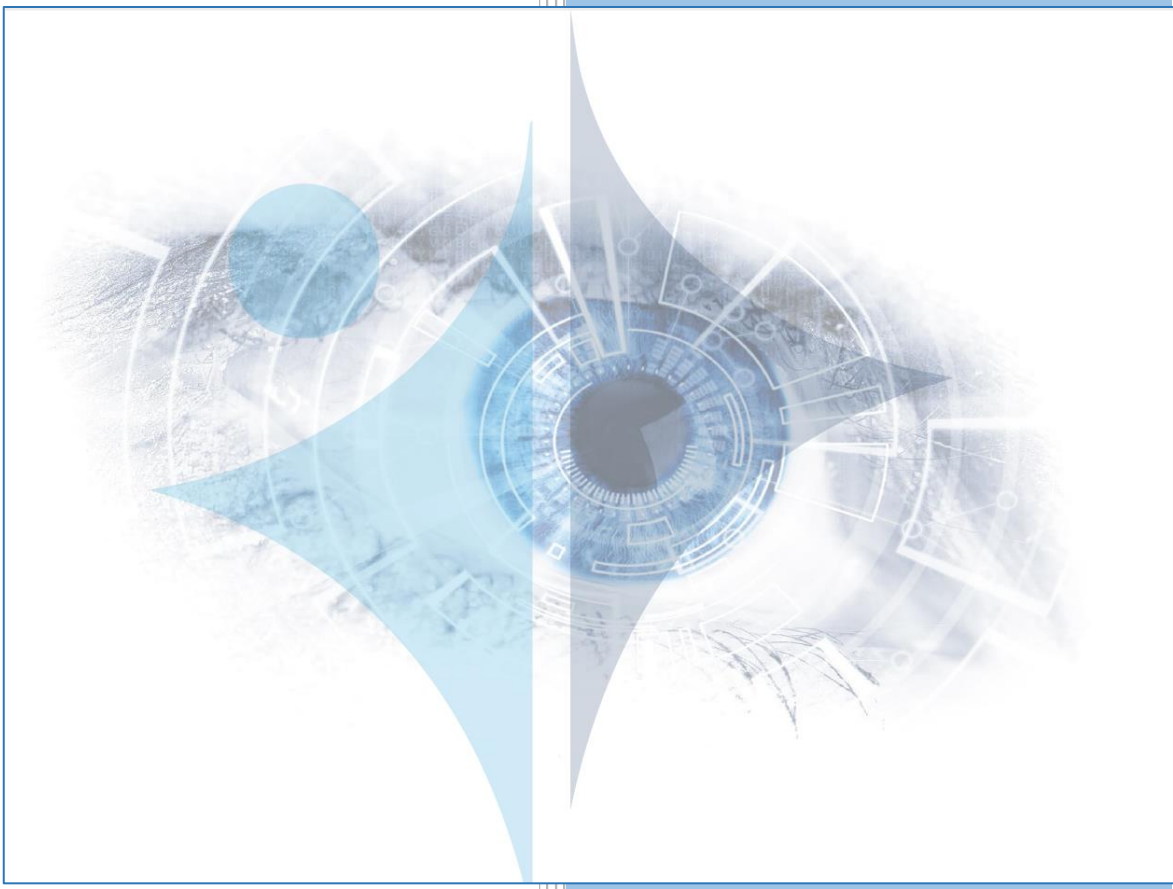
الهيئة الوطنية لحماية المعطيات الشخصية
INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES
NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

Avec le soutien du :

Projet d'appui aux instances indépendantes en Tunisie

Financé par l'Union européenne et le Conseil de l'Europe — UNION EUROPÉENNE — COUNCIL OF EUROPE CONSEIL DE L'EUROPE — Mis en œuvre par le Conseil de l'Europe

RÉFÉRENTIEL RELATIF A LA VIDÉOPROTECTION



www.inpdp.tn

inpdp@inpdp.tn

www.facebook.com/inpdp.tn

www.youtube.com/channel/ucew-cesim0pszpm_xrpjxcia

Mars 2021

1، نهج محمد معلى، ميتوال فيل، 1002، تونس ص.ب. 525
الهاتف (+216) 71 799 853 - 71 799 711 الفاكس 71 799 823

1, Rue Mohamed Moalla, 1002, Tunis, Tunisie B.P. 525
Tél. (+216) 71 799 853 - 71 799 711 Fax 71 799 823

Sommaire

Avant-Propos

Ce référentiel est un ensemble structuré d'informations lié à un domaine, celui de la vidéoprotection, axé sur des questions pratiques et donnant des réponses à des questions que se posent les personnes concernées par cette activité. Il comprend des définitions, des informations, des questions et des solutions que donne l'Instance dans le cadre de sa mission de protection des données personnelles.

L'Instance Nationale de protection des données personnelles est chargée d'après l'article 76 la loi organique numéro 63 du 27 juillet 2004 de la mission entre autres de « … déterminer les garanties indispensables et les mesures appropriées pour la protection des données à caractère personnel … ». C'est dans ce cadre que l'Instance édicte des délibérations qui complètent le cadre juridique constitutionnel, législatif et décrétal dans le domaine de la protection des données personnelles. La délibération relative à la vidéoprotection est celle qui porte le numéro 5 et date du 5 septembre 2018. Ce corpus juridique est accessible en ligne à travers le lien : www.inpdp.nat.tn/Receuil_2019.pdf

Ce référentiel traite de la vidéoprotection. Un phénomène qui prend de l'ampleur dans nos sociétés et auquel recourt aussi bien les particuliers que les structures privées et publiques parfois il est vrai avec une certaine exagération. Ce référentiel répondra aux différents questionnements aussi bien des structures ou personnes qui comptent y recourir que des personnes concernées par ces enregistrements intrusifs de leur vie privée.

Les différents axes de ce référentiel se présentent comme suit :

I. Introduction : public cible, qualification, valeur juridique, terminologie
II. Quelles normes appliquer ?
III. Quelle autorité est compétente ?
IV. Quand y recourir (la finalité) ?
V. Où placer les caméras (le lieu) ?
VI. Comment informer le public ?
VII. Quelle procédure préalable ?
VIII. Quelle durée de conservation ?
IX. Comment protéger les enregistrements ? Comment y accéder et les communiquer, par qui et comment ?
X. Développements récents : Reconnaissance faciale, reconnaissance plaques minéralogique, radar d'excès de vitesse …
XI. Comment porter plaintes en cas de violation des normes ? Quelles sanctions des violations ?

I. Introduction

Pour introduire ce référentiel il est important de déterminer à qui il est destiné (**I.1.**), ainsi que sa valeur juridique (**I.2.**) et la terminologie (**I.3.**) qui y est utilisé. L'introduction se terminera par la manière d'utiliser ce référentiel (**I.4.**).

I.1. Public cible du référentiel

Ce référentiel est conçu pour répondre aux questionnements aussi bien des responsables de traitement qui comptent procéder à l'installation de ces équipements de vidéoprotection et leur conseils juridiques et installateurs ainsi qu'aux personnes qui sont enregistrés dans leur vie quotidiennes par ce procédé intrusif de leur vie privée.

La personne qui recourt à un système de vidéoprotection est considérée de par la loi comme un **responsable de traitement** des données personnelles qui est défini par la loi organique numéro 2004-63 comme étant « … toute personne physique ou morale qui détermine les finalités et les moyens du traitement des données à caractère personnel ». C'est ainsi que la personne physique ou morale de droit privé ou public qui décide de l'installation, de la finalité du recours à ces procédés ainsi que de la manière avec laquelle il va utiliser et traiter les enregistrements issus de ce système et du sort qui leur est réservée. Ce référentiel les guidera dans leur activité pour veiller à ce qu'elle soit en conformité avec les normes.

Ce référentiel est aussi utile aux **installateurs** de ces procédés qui à travers les développements pourront savoir ce qu'il est légalement permis de faire et ce qui est interdit. Ils pourront ainsi conseiller leur client au moment de la conception de l'installation et au cours de l'étape de sa réalisation.

Ce référentiel pourra être utile aux **conseils juridiques** des responsables de traitement qui y trouveront plus clairement explicités les obligations et les procédures à suivre dans les projets d'installation de ces équipements.

D'un autre côté, les **personnes qui sont enregistrés** par ces procédés de protection subissent à cause de ces équipements une intrusion dans leur vie privée. L'Etat doit se porter garant de sa préservation d'après les termes même de la constitution tunisienne. La loi leur attribue des droits que ce référentiel explicite.

I.2. Valeur juridique du référentiel

Ce référentiel se fonde sur le corpus juridique tunisien dans le domaine de la vidéoprotection. Les textes juridiques qui sont détaillés infra sont assez techniques et donc de compréhension difficile. Ce référentiel ne fait que rendre les normes plus accessibles au lecteur. Il permettra ainsi d'éclairer le responsable de traitement sur les bonnes pratiques à suivre lors de l'installation d'un système de vidéoprotection et la manière de l'utiliser par la suite.

Mais ce référentiel n'a ainsi aucune valeur juridique en soi même. Il joue un rôle pédagogique tendant à mieux expliciter les règles à respecter ainsi que la manière avec laquelle on doit exercer ces droits.

I.3. Choix terminologique du référentiel

Dans ce domaine deux termes ont été utilisé dans les textes juridiques comparés et dans la pratique des autorités de protection : vidéo surveillance et plus récemment vidéoprotection. Il est à relever que le terme légalement consacré en Tunisie est celui de vidéosurveillance. Un terme qui est loin d'être adéquat aujourd'hui malgré son utilisation courante depuis 2004. Le terme est concentré sur le qualificatif de la vidéo, qui est la surveillance donnant l'impression que c'est la finalité première de ces systèmes. Ainsi on se rappelait à travers la mise en place de ces systèmes le slogan du Big Brother, « watching you ». Ces équipements ne doivent donc pas contribuer à une mise en place d'une surveillance généralisée.

La lecture de l'article 71 de la loi tunisienne démontre malgré la terminologie utilisée que la finalité de la mise en place de ces installations est loin d'être la surveillance. Aucune fois le terme n'est utilisé. Par contre toutes les finalités avancées indiquent que c'est dans le cadre d'une plus grande consécration de la protection des personnes et des biens. La disposition déclare que « Les moyens de vidéo-surveillance ne peuvent être utilisés que s'ils sont nécessaires pour **assurer la sécurité des personnes**, la **prévention des accidents**, la **protection des biens** ou **l'organisation de l'entrée et de la sortie** de ces espaces ». Toutes les finalités sont ainsi axées sur la manière avec laquelle on peut assurer plus de protection aussi bien des personnes que des biens.

Il est donc impératif de réaliser ce changement important dans la terminologie utilisée. On parlera de ce fait dans ce document de vidéoprotection au lieu de vidéosurveillance.

I.4. Navigation dans le référentiel

Ce référentiel fournira des **informations** concernant le recours à l'utilisation de ces équipements de protection. Il mettra en exergue ce qui devra être respecté comme **obligations légales** aussi bien dans l'installation que dans le traitement des enregistrements collectées. Mais le référentiel déterminera clairement ce qui est **interdit de faire** avec ces installations et fournira quand l'occasion se présente des **conseils** dans ce domaine.

Ces cinq différents développements seront accompagnés par des étiquettes qui permettront d'en distinguer l'objet à travers une identification visuelle :

Information 

Obligation 

Conseil 

Interdiction 

Lien 

II. Le cadre juridique

La vidéoprotection en Tunisie trouve son cadre juridique dans un seul texte juridique en Tunisie : C'est la loi organique numéro 63 du 27 juillet 2004, relative à la protection des données personnelles.

Le législateur considère que la vidéoprotection est avant tout un traitement de données personnelles et que son cadre juridique doit naturellement prendre place dans la loi traitant de leur protection. La vidéoprotection gère des images animées dont les acteurs sont des personnes identifiables à travers leurs caractéristiques physiques, donc biométriques. Ainsi, les enregistrements vidéo rentrent dans le cadre de la définition légale de l'article 4 de la loi organique qui dispose : « … on entend par données à caractère personnel toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement d'identifier une personne physique ou la rendent identifiable ».

Le cadre juridique tunisien de la protection des données personnelles comprend un corpus juridique assez évolué. Ainsi, le premier texte est l'article 24 de la constitution de 2014 qui dispose que « L'État protège la vie privée, l'inviolabilité du domicile et le secret des correspondances, des communications et des données personnelles ». Cet article doit être lié à l'article final du chapitre deux consacré aux droits et aux libertés. Cette disposition clef portant le numéro 49, même si elle s'adresse directement au législateur, elle doit fonder toute action de n'importe quel acteur qui tendrait à limiter les droits des individus. En effet, elle dispose que « … Ces restrictions ne peuvent être établies que pour répondre aux exigences d'un État civil et démocratique, et en vue de sauvegarder les droits d'autrui ou les impératifs de la sûreté publique, de la défense nationale, de la santé publique ou de la moralité publique tout en respectant la proportionnalité entre ces restrictions et leurs justifications … ».

Ce qu'il faut retenir de cette disposition fondatrice, c'est que la vidéoprotection ne peut être mise en place que si elle constitue une limitation nécessaire au droit des individus, celui de se déplacer librement et donc de manière anonyme. Cette limitation doit veiller aussi à être proportionnelle au but recherché et donc non exagéré. Ainsi on ne pourra y recourir qu'en l'absence d'autres systèmes donnant les mêmes résultats et moins intrusifs. Ainsi, si la protection peut être garantie à travers la mise en place d'un système d'alarme contre les intrusions ou de marquage des produits mis en vente pour éviter qu'on les fasse sortir illégalement du local, il faut aller vers ces procédés moins attentatoires aux droits des individus. Une fois la nécessité prouvée, on ne peut ensuite utiliser que les moyens de vidéoprotection adéquats, pertinents et non excessifs pour arriver au but escompté. Ceci se

traduit par une étude préalable pour réduire le nombre de caméras à installer et leur localisation mais surtout décider si on se contente d'un visionnage direct sans enregistrements ou si la sauvegarde est nécessaire et décider du nombre de jours avant leur effacement.

Au-delà de la constitution, le corpus juridique tunisien a principalement mis en place trois textes juridiques formels qui encadrent la vidéoprotection :

- La **loi organique n° 63 du 27 Juillet 2004** relative à la protection des données personnelles qui a réservé une section IV du chapitre V à la vidéoprotection : Elle comprend les articles 69 à 74.
- Le **décret n° 2007-3004 du 27 novembre 2007** qui encadre la demande d'autorisation préalable à introduire auprès de l'INPDP pour l'installation d'un système de vidéoprotection.
- La **délibération de l'Instance nationale de protection des données personnelles numéro 5 datée du 5 septembre 2018** qui a déterminé les conditions et procédures relatives à la protection des données personnelles dans le cadre de la vidéoprotection.

Tous ces textes sont accessibles dans un recueil mis à jour accessible sur le site de l'Instance nationale de protection des données personnelles à l'adresse actuelle : www.inpdp.nat.tn/Receuil_2019.pdf.

III. L'autorité compétente

La seule autorité compétente pour autoriser et contrôler le recours à la vidéoprotection en Tunisie est l'Instance nationale de protection des données personnelles. Elle bénéficie d'une compétence exclusive dans ce domaine qui lui permet de réaliser, sous le contrôle du juge, les opérations suivantes :

- Détermine les modalités d'installation et de traitement des données issues de la vidéoprotection ;
- Autorise l'installation de ces systèmes de vidéoprotection ;
- Statue sur les litiges ou plaintes contre des installations non conformes et contrôle la conformité de ces traitements aux normes.

III.1. Détermine les modalités

L'article 76 de la loi organique attribue à l'INPDP entre autre mission générale de « déterminer les garanties indispensables et les mesures appropriées pour la protection des données à caractère personnel » et d' « élaborer des règles de conduite relatives au traitement des données à caractère personnel ».

C'est dans ce cadre que l'Instance, dans les limites de ce qui a été prévu dans la loi et les décrets d'application, se trouve amené à élaborer les normes de protection pratiques dans les différents domaines. Celles-ci découlent des questionnements que l'instance reçoit de la part des responsables de traitement dans le cadre des demandes d'avis qui lui sont officiellement adressées. L'Instance joue aussi un rôle de veille sur le plan international en essayant d'étudier les meilleures pratiques et de réunir les normes comparées mises en place dans les expériences internationales. C'est à travers ces actions que l'Instance édicte ces délibérations qui constituent la consécration de son pouvoir réglementaire consacré par l'article 76. Cet acte constituant un acte administratif d'une structure publique, s'il pose un problème de légalité, il est susceptible de recours en excès de pouvoir devant le Tribunal administratif.

Sur la base de ce pouvoir réglementaire, l'Instance a édicté une délibération qui est relative à la vidéoprotection en date du 5 septembre 2018 : www.inpdp.nat.tn/5_VS.pdf

III.2. Autorise l'installation

Le même article 76 de la loi organique prévoit que l'INPDP a la mission d'« accorder les autorisations, recevoir les déclarations pour la

mise en œuvre du traitement des données à caractère personnel, ou les retirer dans les cas prévus par la présente loi ».

D'un autre côté l'article 69 de la même loi dispose que « … l'utilisation des moyens de vidéo-surveillance est soumise à une autorisation préalable de l'Instance Nationale de Protection des Données à Caractère Personnel ».

Ensuite le décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel confirme cela dans son article 10 en déclarant « Avant l'utilisation de moyens de vidéo-surveillance, une autorisation doit être obtenue de l'instance nationale de protection des données à caractère personnel ».

III.3. Reçoit les plaintes et vérifie la conformité

La troisième mission dont est chargé l'Instance nationale de protection des données personnelles dans ce domaine est de « recevoir les plaintes portées dans le cadre de la compétence qui lui est attribuée en vertu de la présente loi » et donc dans le domaine de la vidéoprotection.

Toute personne qui subit une violation des normes dans l'installation et le traitement des données de vidéoprotection est habilitée à saisir l'INPDP.

L'Instance, dans le cadre des pouvoirs qui lui sont accordées peut « accéder aux données à caractère personnel faisant l'objet d'un traitement afin de procéder à leur vérification … ».

Sur la base de son évaluation de la conformité ou non de l'installation aux normes, l'Instance peut être emmené à retirer l'autorisation accordée et s'il le faut transférer le dossier de violation la loi au procureur de la république compétent.

L'article 81 de la loi organique dispose dans ce sens que « L'instance peut décider après audition du responsable du traitement ou du sous-traitant de retirer l'autorisation … ».

IV. La finalité de l'installation

L'installation d'un système de vidéoprotection est une atteinte à la vie privée des individus qui sont enregistrés dans leurs déplacements et activités par les caméras sans qu'ils soient parfois vraiment conscients de leur existence ni réconforté sur le sort qui sera réservé à ces vidéos.

C'est pour cette raison que le législateur a limité le but du recours à ces installations de manière explicite dans la loi organique numéro 63 de 2004.

En effet, l'article 71 de la loi organique 63-2004 qui a été repris par l'article 2 de la délibération numéro 5 de l'Instance limite les finalités du recours à ces installations à quatre. L'article est clairement rédigé dans ce sens puisqu'il dispose que « … les moyens de vidéoprotection ne doivent être utilisés que pour les finalités suivantes : … ». Ainsi la liste qui suit est limitative et ne peut souffrir d'extension possible si on veut rester en conformité avec la volonté du législateur.

Ces quatre finalités sont celles permettant d'assurer :

- La sécurité des personnes ;
- La prévention des accidents ;
- La protection des biens ;
- L'entrée et la sortie des espaces.

IV.1. La sécurité des personnes

La finalité relative à la sécurité des personnes porte sur toutes les installations de système de vidéoprotection tendant à protéger les individus afin d'en assurer la sécurité physique.

Cela peut avoir aussi pour finalité de les prémunir contre les agressions, et si cela se produit, de pouvoir déterminer l'identité de leur auteur.

La protection peut aussi toucher, dans des crèches ou des établissements de loisirs pour jeunes, des enfants qui peuvent se faire mal ou faire mal à un congénère ou subir des mauvais traitements de la part d'adultes ou de malfaiteurs dans les abords de leur établissement.

La protection à travers des systèmes vidéo peuvent permettre de suivre visuellement un nombre important de patients dans des salles de réanimations par un seul médecin et même à distance.

Installé dans des lieux de détention, les systèmes de vidéoprotection permettent d'éviter les agressions entre les colocataires de ces espaces.

Ils peuvent aussi servir à éviter que des personnes en situation psychologique instable ne se fassent mal dans des établissements de santé ou dans des cellules de détention.

C'est aussi le cas des systèmes de vidéoprotection mis en place par les autorités publiques sur la voie publique et qui permettent de dissuader les délinquants et les criminels de réaliser leurs méfaits contre des personnes.

Les caméras piétons portés par les agents publics permettent de dissuader les personnes avec lesquelles elles sont en contact de les agresser verbalement ou physiquement puisqu'elles savent qu'elles sont filmées.

IV.2. La prévention des accidents

Les systèmes de vidéoprotection peuvent être installés dans les endroits ouverts au public ainsi que sur la voie publique en vue de prévenir la survenance d'accidents en dissuadant des comportements irresponsables de la part des usagers de certains espaces et en cas d'accident identifier les responsables.

Les situations où des systèmes de vidéoprotection sont installés peuvent être les :

- Croisements sur la voie publique pour gérer la circulation mais surtout assurer la sécurité des piétons et des automobilistes ;
- Manèges et foires et espaces de jeux présentant un danger ;
- Manifestations sportives et culturelles en présence d'un grand nombre de spectateurs cohabitant dans un espace relativement réduit ;
- Les espaces ouverts au public

IV.3. La protection des biens

Les systèmes de vidéoprotection sont utiles pour protéger les biens qu'ils soient mobiliers ou immobiliers et spécialement contre :

- Le vandalisme des bâtiments ;
- La détérioration des équipements collectifs ou privées ;
- Le vol ;
- L'intrusion ;
- L'usage illégal de certaines installations …

IV.4. L'entrée et la sortie des espaces

L'entrée et sortie des bâtiments ouverts au public et aux usagers constituent des endroits stratégiques qui permettent d'identifier les risques d'encombrement et surtout de réguler le trafic et de prendre les mesures nécessaires pour mettre en place le personnel nécessaire à la gestion du taux de fréquentation.

Ces systèmes de vidéoprotection peuvent ainsi être installés dans les entrées et sortie des espaces suivants :

- Les centres commerciaux ;
- Les espaces de loisir ;
- Les établissements d'enseignement ;
- Les structures de santé ;
- Les administration et services publics …

Le responsable de traitement qui procède à la mise en place d'un système de vidéoprotection ne peut le faire pour une autre finalité que celles indiquées. C'est sur quoi insiste l'article 71 de la loi qui cite ces espaces de manière limitative et donc non extensible.

Le responsable de traitement doit aussi indiquer clairement cette finalité dans la demande d'autorisation qu'il soumet à l'évaluation de l'Instance. Celle-ci figurera dans la décision d'autorisation délivrée par l'INPDP et devra être respectée tout au long de la durée de traitement des enregistrements s'il a été décidé et autorisé d'y procéder.

La finalité du traitement va permettre aussi de décider si la vidéoprotection se contentera d'une visualisation en temps réel ou procédera à l'enregistrement et la sauvegarde de ces vidéos. Le principe de la minimisation des données oblige en effet de se contenter de la visualisation directe sans besoin de sauvegarder les vidéos quand cela répond amplement à la finalité arrêtée.

V. Le lieu de l'installation

Les équipements de vidéoprotection ne peuvent être installés que dans les endroits prévus par la loi. La liste des espaces qui peuvent être vidéos protégés est définie par la loi organique de 2004 et elle est de ce fait limitative.

La norme à appliquer quel que soit l'installation d'un système de vidéoprotection est qu'il ne doit pas couvrir des espaces privées ou intimes à l'occasion de la protection d'autres espaces généralement ouverts au public.

V.1. Les lieux ouverts au public et leurs entrées

Tout espace ouvert au public et donc qui permet à des usagers ou des clients de s'y trouver peut justifier la mise en place pour cette seule raison des systèmes de vidéoprotection. Les espaces eux-mêmes peuvent être vidéoprotégées ainsi que leurs entrées et sortie.

Font partie de ces espaces :

- Les commerces ;
- Les administrations ;
- Les établissements hospitaliers et de santé ;
- Les banques, assurances ;
- Les structures de services ;
- Les espaces de spectacle et de loisir ;
- Les cafés et les restaurants …

V.2. Les espaces et moyens de transport

Tous les espaces en relation avec le transport peuvent être couverts par des systèmes de vidéoprotection.

Ce sont :

- Les ports ;
- Les aéroports ;
- Les gares de train ou de bus ;
- Les stations de bus ou de taxis individuels ou collectifs ;
- L'intérieur des moyens de transport ;
- Les péages des autoroutes ;
- Les routes, voies ferrées ...

V.3. Les espaces de travail collectifs

Les espaces de travail collectifs sont ceux où travaillent normalement plus d'une personne. Cette règle est ainsi consacrée car elle permet d'assurer la sécurité de cet espace sans toucher à l'intimité de son occupant. En effet, dans un bureau individuel quand la porte est fermée son occupant se considère dans un espace privée qu'une caméra de protection violerait l'intimité.

Il est donc interdit pour un employeur d'installer une caméra de protection dans un bureau individuel.

Mais la pratique et les besoins a emmené l'Instance à élargir le champ d'application de cet article en respectant la motivation du législateur dans son œuvre de limitation des espaces d'installation des caméras de protection. La jurisprudence de l'Instance a permis ainsi l'installation de ces systèmes dans les entrées et sorti des espaces de travail, les couloirs et espaces de dégagements, les dépôts et les chaines de production.

Par contre, l'INPDP a toujours refusé l'installation de ces équipements en

plus des bureaux individuels dans les cantines, les espaces de repos ou de loisirs réservés aux employés, dans les salles de réunion ou de conseil ; Ces endroits nécessitent une certaine intimité ou secret incompatible avec une vidéoprotection qui passe dans la quasi-totalité des cas par un enregistrement des vidéos.

Si la loi et la jurisprudence de l'INPD autorisent l'installation des équipements dans les espaces de travail collectif, il est légitime pour un employé de refuser l'orientation volontaire de la caméra par son employeur sur sa personne ou sur l'écran de son ordinateur. Cela dépasserait la vidéoprotection pour constituer une situation d'harcèlement et de surveillance exagérée.

V.4. Les espaces non privatifs des habitations collectives

Quand les espaces à protéger font partie d'une propriété collective, elles peuvent être vidéoprotégées. Ces espaces doivent faire partie des espaces collectifs et non privatifs. Cela couvre les espaces suivants :

- Les espaces collectifs tel que les hall, couloirs, locaux de vélos ou poussettes, cour intérieure, jardin communs et aires de jeu …
- Les ascenseurs ;
- Les parkings

La règle est que le champ de vision des caméras ne doit pas inclure des es-

paces privatifs tel que des jardins ou terrasses ou encore des balcons et même des ouvertures (fenêtres et baies vitrées) qui permettent de filmer l'intérieur de l'habitation … II est de même non permis de couvrir par

les caméras les portes d'entrée des appartements et les couloirs menant à une seule entrée d'appartement.

Dans tous les cas l'installation de ces équipements de vidéoprotection ne peut être autorisé si elle n'est pas permise par l'assemblée générale des copropriétaires et si un syndic n'est pas constitué par un document d'acceptation par tous les copropriétaires ou les propriétaires d'un lotissement avec une voie privative.

V.5. Les espaces réservés à l'éducation et l'enseignement

Les espaces réservées à l'éduction et à l'enseignement sont considérées en même temps comme des espaces ouverts au public et comme des espaces de travail collectif. Une caméra de vidéoprotection ne peut être installé pour servir à contrôler et surveiller des apprenants ou des enseignants.

La règle est que ces installations ne doivent ni s'immiscer dans l'intimité de la relation enseignant apprenant ni toucher à l'intimité des apprenants. Il n'est pas de ce fait permis de vidéoprotéger :

- Les classes et espaces d'enseignement ;
- La cour de récréation ;
- Les préaux ;
- Les cantine ;
- Les dortoirs …

Pour ce qui est des espaces d'enseignement, la jurisprudence de l'INPDP a permis d'y installer des systèmes de vidéoprotection dans des situations particulières : Quand les caméras sont orientées exclusivement vers des équipements onéreux dans le but d'éviter le vandalisme ou le vol.

Les équipements de vidéoprotection peuvent être autorisées s'ils couvrent les espaces suivants :

- Les halls d'entrée ;
- Les couloirs ;
- Les bibliothèques ;
- Les abords extérieurs directs de l'établissement surtout pour ceux accueillants des enfants.

V.6. Les établissements de santé

Les établissements de santé sont aussi nombreux que variés. On peut citer principalement les hôpitaux, cliniques, centre de dialyse, laboratoires d'analyse, centres d'imagerie … ainsi que les cabinets de médecins de libre pratique.

Il est légitime, comme dans tout espace ouvert au public d'installer des caméras de vidéoprotection aux entrées et sorties du bâtiment afin de pouvoir déterminer en cas de besoin les personnes qui entrent et quittent les lieux.

Il en est de même pour les couloirs et les ascenseurs ainsi que les zones de chargement qui peuvent être couverts par des équipements de vidéoprotection afin de contrôler le flux d'activité de l'établissement. Il est important même d'installer des équipements de vidéoprotection à l'entrée des zones réglementées avec pour finalité de s'assurer que seules les personnes autorisées y aient accès.

A l'image de tous les espaces intimes il est interdit de vidéoprotéger les lits occupés par des patients. Il n'est ainsi pas permis de recourir à ces équipements dans les unités de réanimation ou de soins intensifs. L'exception qui a été permise par l'INPDP en se basant sur la nécessité et la proportionnalité et spécialement au moment de la lutte contre le Covid-19 c'est que ces équipements pouvaient être installées pour contrôler l'état des patients mais à condition que cela ne permette pas l'enregistrement mais seulement le visionnage en temps réel des vidéos par des médecins ou du personnel paramédical.

Le cabinet médical d'un médecin de libre pratique est considéré comme un lieu ouvert au public. Le responsable de traitement, en l'occurrence le médecin, doit se limiter à installer des équipements de vidéoprotection à l'entrée, l'accueil ou la salle d'attente, jamais dans la salle de consultation qui est couverte par le secret.

Il devra en outre informer ses patients de façon claire et permanente de l'existence d'un système de vidéoprotection, par exemple en disposant d'un affichage à l'entrée du cabinet et dans la salle d'attente.

V.7. Les espaces privatifs de liberté

L'installation de vidéoprotection dans ces lieux ne se justifie que pour la protection et la sécurité des agents de police et des détenus et des personnes en garde à vue.

Les lieux autorisés à installer la vidéoprotection sont :

- Les abris de transport ;
- Les couloirs des visiteurs ;
- Les couloirs menant aux entrées des bâtiments pénitentiaires et centres de détention ;
- Les salles de réception ;
- Les salles d'attentes ;

- Les espaces communs des détenues ;
- Les espaces dédiés au travail artisanal et au divertissement des détenus ;
- Les façades des bâtiments pénitentiaires et centre de détention ;

Par exception, et de manière limitative certains lieux sont autorisés à être filmés par vidéoprotection à condition que la visualisation se fasse qu'en temps réel et sans enregistrement vidéo :

- Les chambres d'isolement ;
- Les détenus présentant des symptômes de maladie neurologiques ou psychologiques ;
- Les espaces de couchage et lieux destinés à interroger les détenus ou les prisonniers en garde à vue pour leur protection ;
- Les espaces réservés aux visites des détenus et leur entretient avec leurs avocats.

V.8. La voie publique

Il est interdit que toutes les caméras mises en place pour protéger des espaces prévues dans les développements précédents ne permettent de couvrir même des portions minimes de la voie publique. Cette interdiction ne souffre d'aucune exception et se trouve généralisé dans les législations comparées.

Seules certaines autorités publiques, dans le cadre de leur mission d'assurer la sécurité publique, ont le droit de vidéoprotéger la voie publique. Cela découle de la nature même des missions déterminées par la loi pour les autorités suivantes :

- Le ministère de l'intérieur sur tout le territoire national ;
- Le ministère de la défense dans les espaces militaires ou mises sous son contrôle ainsi que l'environnement direct des installations militaires ;
- Les collectivités locales pour les espaces publics dans la circonscription de la commune.

Des caméras peuvent être installées sur la voie publique pour prévenir des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ou des actes de terrorisme

Ni les entreprises, ni les établissements publics ne peuvent vidéoprotéger la voie publique. Ils peuvent exceptionnellement filmer les abords immédiats de leurs bâtiments et installations (la façade extérieure par exemple mais pas

la rue en tant que telle) dans les lieux susceptibles d'être exposés à des actes de banditisme, de terrorisme ou de vandalisme. C'est aussi le cas pour les espaces stratégiques dépendants par exemple les abords des banques, des champs pétrolifères et les bâtiments de souveraineté comme les ministères.

V.9. Les caméras piétons

Dans les expériences comparées, les caméras piétons sont un équipement léger portées à la poitrine ou l'épaule par des agents publics afin d'enregistrer les interactions avec les usagers généralement du service public ou le public. Ces caméras constituent une exception axiale de la vidéoprotection car elles permettent l'enregistrement des images mais aussi le son. Cette exception va

à l'encontre de ce que dispose l'alinéa deux de l'article 71 que dispose que « les enregistrements vidéo ne peuvent être accompagnés d'enregistrements sonores ».

Les finalités de recours à ces équipements sont la prévention des incidents au cours des interventions des agents et le constat des infractions et la poursuite de leurs auteurs mais aussi collecter des données vidéos dans le cadre de la formation des agents.

En Tunisie, c'est la douane qui a demandé l'avis de l'Instance autour du projet d'équipement des douaniers au port de la Goulette de caméras piétons pour la campagne de retour des tunisiens à l'étranger au pays au cours de l'été 2018.

L'Instance a indiqué que même si aucune disposition légale n'encadre ces équipements de vidéoprotection il est conseillé de respecter certaines règles qui découle du régime général prévu dans la loi de 2004 : Il est impératif d'informer les personnes concernées de l'existence de ces finalités et de leur finalité, préserver les enregistrements et les sécuriser afin d'éviter leur communication au tiers, n'en donner l'accès qu'aux seules personnes qui y sont habilités de par leurs attributions ou pour les besoins de procédures juridictionnelles.

L'INPDP a introduit dans le nouveau projet de loi sur la protection des données personnelles des dispositions encadrant le recours à ces nouveaux équipements.

V.10. Les espaces privées

Toute personne peut installer des systèmes de vidéoprotection dans les espaces qui lui appartiennent et qui ne sont pas ouverts au public. C'est le cas d'une habitation, d'une exploitation agricole mais aussi d'un véhicule.

Le champ de vision des équipements ne doit couvrir ni les espaces appartenant à des voisins ni la voie publique même si c'est pour assurer la sécurité de leur véhicule garé devant leur propriété.

Dans ce cas spécifique la personne qui procède à cette installation dans sa propriété doit impérativement informer les éventuels visiteurs et le personnel domestique de l'existence de ces équipements par une pancarte visible aux entrées de la propriété. Mais n'étant pas un espace ouvert au public, il est dispensé d'obtenir une autorisation préalable de l'INPDP.

VI. L'information du public

L'article premier de la loi organique numéro 63 relative à la protection des données personnelles dispose que les données personnelles « … ne peuvent être traitées que dans le cadre de la transparence, la loyauté … ». Ceci implique que les traitements dont la collecte de données doit être connue des personnes concernées. C'est ce qui fonde l'illégalité des équipements cachées.

L'article 72 de la même loi dispose clairement que « Le public doit être informé d'une manière claire et permanente de l'existence de moyens de vidéo-surveillance ».

Le traitement des données personnelles devant obtenir un consentement préalable des personnes concernées, celui-ci ne peut être obtenu de la part de personnes accédant à un espace vidéoprotégé. C'est la délibération de l'INPDP numéro 5 en date du 5 septembre 2018 relative à la vidéoprotection qui consacre des développements dans son article 17 sur la manière d'informer le public. Il y est disposé que : « Le responsable de traitement doit informer le public de l'existence d'équipements de vidéoprotection à travers une affiche à l'entrée du bâtiment ou de l'espace qui soit visible et claire et portant les mentions suivantes :

- L'existence des équipements de vidéoprotection ;
- Le numéro et la date de l'autorisation de l'INPDP ;
- L'identité et la qualité du responsable de traitement ;
- Les coordonnées pour exercer le droit d'accès (Adresse physique ou postale ou électronique ou numéro de téléphone) ;

Ci-joint un modèle d'affichette qui pourrait informer suffisamment le public sur l'existence de l'installation et sur la légalité du traitement et lui permettre d'avoir les contacts nécessaires pour exercer son droit d'accès.

ESPACE SOUS VIDÉOPROTECTION

Loi organique 2004-63 (Articles 69 à 74)

Autorisation INPDP :

Pour toute demande d'accès aux images :

VII. Les enregistrements vidéo

Les aspects intrusifs dans la vidéoprotection est surtout le fait que les équipements captent les photos et comportement des individus mais surtout qu'il en garde une trace. C'est pour cette raison que l'installation doit répondre impérativement à deux questions importantes : Est-il nécessaire d'enregistrer les vidéos et combien de temps peut-on les garder ?

La réponse à ces questionnements doit prendre en considération l'impératif consacré dans l'article 49 de la constitution suivant lequel les limites aux droits et libertés des individus doit se conformer à la règle de la proportionnalité. Un principe qui prendra place dans les règles de protection des données personnelles sous la dénomination de minimisation des données collectées. Les données ne peuvent en effet être collectées que pour répondre strictement et pas plus à la finalité de traitement. Mais la loi interdit clairement certains enregistrements.

VII.1. L'interdiction de l'enregistrement audio

Les enregistrements vidéo ne peuvent contenir en plus de l'image, le son. La loi organique numéro 63 relative à la protection des données personnelles est claire sur cette interdiction qui est reprise par l'article 3 de la délibération numéro 5 de l'INPDP.

Le paragraphe deux de l'article 71 de la loi organique numéro 63 dispose clairement que « … les enregistrements vidéo ne peuvent être accompagnés d'enregistrements sonores ».

L'Instance n'a jamais autorisé d'exception à cette interdiction du fait que rien à son avis ne justifierais une plus grande intrusion dans la vie privée des individus.

En Tunisie aucun texte général ne sanctionne l'enregistrement des paroles d'un individu sans son consentement. En France, l'enregistrement audio est sanctionné par l'article 226-1 du code pénal comme une atteinte à la vie privé car capter, enregistrer ou transmettre des paroles prononcées à titre privé ou confidentiel sans le consentement de l'auteur est passible de 45 000 euros d'amende et d'un an de prison.

Par contre l'article 87 de la loi organique numéro 63 dispose qu'est « puni d'un emprisonnement de deux ans et d'une amende de dix mille dinars, celui qui viole les dispositions de l'article … 71 de la présente loi », ce qui inclus l'enregistrement du son dans un système de vidéoprotection.

VII.2. Enregistrement ou visualisation en temps réel

L'installation du système de vidéoprotection peut ne pas recourir à l'enregistrement. Si la finalité peut être atteinte sans enregistrer les vidéos mais seulement en permettre la visualisation en temps réel, l'intrusion dans la vie privée des individus est minimisée. Dans ce cas le procédé ne fait que délocaliser l'œil d'un agent de sécurité de l'espace protégé vers une salle de contrôle à distance. C'est une situation similaire à celle où la personne est présente sur les lieux afin de surveiller les mouvements ou actions des personnes présentes et intervenir en lançant une alerte ou en guidant des collègues pour une intervention sur le terrain. Un responsable d'une chaine de production peut visualiser en temps réel sur son téléphone portable les vidéos d'une salle de production pour s'assurer, sans être obligé de se trouver sur place, si le travail se fait normalement et éventuellement intervenir par téléphone pour donner des consignes ou des ordres.

La vidéoprotection n'entraine ainsi pas nécessairement de l'enregistrement et dans ces cas l'intrusion dans la vie privée des individus est minimisé au maximum et surtout écarte le risque de voir des enregistrements fuiter ou diffusé en dehors du système ou transmises à des tiers.

L'absence d'enregistrement permet aussi de vidéo surveiller des espaces où il n'est pas permis d'installer des systèmes de vidéoprotection dotées de l'enregistrement comme c'est le cas des espaces intimes ou assimilés. C'est la justification qui a permis à l'instance d'autoriser l'installation de ces systèmes sans enregistrement dans les dortoirs ou les salles de visites des institutions carcérales ou les salles de réanimation et de soins intensifs dans les institutions de santé. Dans ces cas le gardien de prison ou le personnel médical bénéficie seulement d'une délocalisation simple de leur œil.

C'est ce qui concrétisé par l'article 16 de la délibération numéro 5 relative à la vidéoprotection. Il dispose que « Le responsable de traitement, selon la situation et après avoir obtenu l'autorisation de l'INPDP, peut se limiter à une visualisation des images captées par l'objectif des caméras installés mais sans les enregistrer, répondant ainsi aux spécificités de l'espace où l'enregistrement est réalisé : un dortoir collectif, des espaces pénitentiaires ou de détention provisoire ou encore des espaces de soins intensifs dans les établissements de santé ».

VII.3. Durée de conservation des enregistrements

Une des règles de la protection des données personnelles est que les données personnelles ne peuvent être gardées par le responsable de traitement que

le temps nécessaire à la réalisation de la finalité du traitement. C'est ce qu'affirme clairement l'article 45 de la loi organique numéro 63 de 2004 en disposant que « Les données à caractère personnel doivent être détruites … en cas de réalisation des finalités pour lesquelles elles ont été collectées ... ».

La règle est reproduite dans le domaine de la vidéoprotection par l'article 74 qui stipule que « Les enregistrements vidéo doivent être détruits lorsqu'ils ne sont plus nécessaires à la réalisation des finalités pour lesquelles ils ont été effectués ou lorsque l'intérêt de la personne concernée exige sa suppression à moins que ces enregistrements ne s'avèrent utiles pour la recherche et les poursuites d'infractions pénales ».

La jurisprudence de l'INPDP a fixé à l'image de toutes les autorités de protection la durée maximale de sauvegarde des enregistrements : la durée maximale ne peut excéder trente jours mais peut être limitée par exemple à seulement huit jours. La détermination de la durée de conservation des enregistrements est justifiée par le responsable de traitement au moment de la demande de l'autorisation auprès de l'INPDP.

L'INPDP a consacré cette norme dans l'article 18 de la délibération numéro 5 en date du 5 septembre 2018. Il dispose que « La conservation des enregistrements expire avec la réalisation de la finalité pour laquelle les moyens de vidéoprotection ont été installés et, dans tous les cas, ne peut être prolongé au-delà de trente jours qu'avec l'autorisation exceptionnelle de l'Instance.

Le système de vidéoprotection doit être programmé de manière à ce que ces enregistrements soient automatiquement supprimés à l'expiration de la période de conservation, dans le cadre de ce que permettent les caractéristiques techniques de l'équipement utilisé ».

Il est à rappeler à ce propos que conserver les images quelques jours suffit à effectuer les vérifications nécessaires en cas d'incident et permet d'enclencher d'éventuelles procédures pénales ou disciplinaires. Si de telles procédures sont engagées, les images sont alors extraites du dispositif (après consignation de cette opération dans un registre spécifique) et conservées pour la durée de la procédure.

VIII. L'autorisation préalable

L'installation d'un système de vidéoprotection est soumise d'après la loi et en des termes clairs à une autorisation préalable de la part de l'Instance nationale de protection des données personnelles.

L'article 69 de la loi organique numéro 63-2004 dispose que « … l'utilisation des moyens de vidéo-surveillance est soumise à une autorisation préalable de l'Instance Nationale de Protection des Données à Caractère Personnel ».

Le décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel dans son article 10 dispose qu' « Avant l'utilisation de moyens de vidéo-surveillance, une autorisation doit être obtenue de l'instance nationale de protection des données à caractère personnel ».

Ainsi aucune exception ne peut permettre de dispenser de l'obtention d'une autorisation de l'Instance. Cette demande est d'après les textes préalables à l'installation des équipements.

Elle doit être introduite auprès de l'Instance à travers le formulaire mis en ligne sur le site de l'instance à travers le lien suivant : www.inpdp.nat.tn/video.pdf. Il est annexé au présent référentiel

L'article 14 de la délibération numéro 5 de l'INPDP détermine les conditions de présentation de la demande d'autorisation. Elle doit informer sur les points relatifs à l'installation et respecter les procédures suivantes :

- Le formulaire doit être rempli et signé par le responsable de traitement qui a décidé de recourir à ces équipements ainsi que la finalité de leur utilisation ;
- La finalité du recours à la vidéoprotection ;
- Déterminer le nombre de caméras en spécifiant si elle est fixe ou mobile, intérieure ou extérieure et son champ de vision et l'espace vidéoprotégé ;
- La description des mesures de sécurité mises en place pour assurer la confidentialité des enregistrements ;
- La manière avec laquelle on informe le public des installations ;
- La garantie d'exercice du droit d'accès aux personnes intéressées par les enregistrements ;
- La détermination de la durée des enregistrements ;

- Joindre à la demande un schéma ou plan de l'installation portant le tampon du responsable et sa signature et permettant de localiser les caméras, leur orientation et leurs champs de vision.

L'Instance reçoit ces demandes d'autorisation suivant l'un des canaux suivants :

- Déposé au siège de l'instance contre récépissé ;
- Par mail à l'adresse officielle de l'Instance ;
- Par courrier postal adressé à l'Instance.

L'Instance traite le dossier de la demande et le secrétariat peut recontacter le responsable de traitement pour compléter son dossier et éviter son report suite à la réunion du conseil.

Il revient en effet à l'Instance d'après l'article 76 de la loi organique numéro 63 de 2004 d' « … accorder les autorisations, recevoir les déclarations pour la mise en œuvre du traitement des données à caractère personnel, ou les retirer dans les cas prévus par la présente loi … ». Ce qui veut dire que c'est le conseil de l'Instance qui prend la décision d'accorder ou refuser l'autorisation, il lui est possible aussi de reporter sa décision jusqu'à réception de plus amples informations de la part du responsable de traitement.

Les décisions d'accorder ou de refuser l'autorisation est portée à la connaissance du responsable de traitement et le texte de la décision lui est remise contre décharge au siège de l'Instance.

Le responsable de traitement doit respecter les termes et conditions de l'autorisation. S'il s'avère qu'il a modifié son installation en ajoutant des caméras ou leur orientation sans en avertir l'Instance et si l'instance constate que ces faits sont de nature à violer les droits des individus ou la loi, l'Instance peut à travers une décision de son conseil décider le retrait motivé de l'autorisation accordée.

Toutes les décisions de l'Instance que ce soit d'autorisation ou de refus de d'autorisation ou de retrait de décision préalable sont susceptibles de recours en appel devant la cour d'appel de Tunis et ce conformément à l'article 82 de la loi organique numéro 63-2004 qui stipule que : « … Les décisions de l'Instance sont susceptibles de recours devant la cour d'appel de Tunis dans un délai d'un mois à partir de leur notification. Il est statué sur le recours selon les dispositions du Code de procédure civile et commerciale.

Les décisions de l'Instance sont exécutées nonobstant le recours formulé à leur encontre. Le premier président de la cour d'appel de Tunis peut ordonner en référé la suspension de leur exécution jusqu'à ce qu'il soit statué sur le recours lorsque cette exécution est susceptible de causer un préjudice irréversible. La décision ordonnant la suspension n'est susceptible d'aucune

voie de recours. La cour saisie de l'affaire doit statuer sur le recours dans un délai ne dépassant pas trois mois à compter de la date de sa saisine ».

IX. La protection et la communication des vidéos

Le responsable de traitement doit conformément à une obligation générale prendre toutes les mesures nécessaires à la préservation de la sécurité et de la confidentialité des données collectées et traitées. L'article 18 de la loi organique numéro 63-2004 dispose que « Toute personne qui effectue, personnellement ou par une tierce personne, le traitement des données à caractère personnel est tenue à l'égard des personnes concernées de prendre toutes les précautions nécessaires pour assurer la sécurité de ces données et empêcher les tiers de procéder à leur modification, à leur altération ou à leur consultation sans l'autorisation de la personne concernée ».

Pour ce qui est du cadre spécifique de la vidéoprotection, l'article 19 de la délibération numéro 5 de l'INPDP relative à ce traitement déclare que : « Le responsable de traitement prend toutes les mesures nécessaires pour garantir la sécurité et la confidentialité des données contenues dans les enregistrements et leur intégrité et empêcher quiconque de les consulter, d'y apporter des modifications ou de leur porter atteinte.

Les enregistrements collectés doivent être stockés dans des espaces sécurisés qui sont localisés dans des espaces fermés et protégés, auxquels seules les personnes autorisées peuvent accéder.

Le responsable du traitement doit tenir un registre spécial qui comprend l'identité de la personne qui accède aux enregistrements ainsi que la date et l'heure de chaque opération et sa référence ».

L'installation d'un système de vidéoprotection oblige ainsi tout responsable de traitement de respecter les obligations suivantes :

- Prendre toutes les mesures techniques et organisationnelles appropriées et disponibles, afin de garantir un niveau de sécurité adapté au risque ;
- Limiter l'accès aux enregistrements au personnes qui de par leur fonction ou qualité sont habilités à le faire : responsable de la sécurité de l'organisme, gardiens d'un espace, syndic ou membres du Conseil syndical d'habitation collective, direction d'un commerce … ;
- Former et sensibiliser les personnes habilitées à consulter les images aux règles de mise en œuvre d'un système de vidéoprotection et leur faire signer une charte de confidentialité ;
- Si les images sont accessibles à distance, depuis internet sur un téléphone mobile par exemple, il faut sécuriser cet accès par un mot de passe robuste, en utilisant une connexion https et éventuellement en recourant au cryptage des vidéos et surtout éviter de recourir à l'enregistrement … ;

- Limiter la consultation des images au cas d'incident (vandalisme, dégradation, agression, etc.). Elles ne peuvent servir à « surveiller » les allées et venues des résidents ou des visiteurs ou des employés ;

Si le responsable de traitement est emmené à communiquer les vidéos enregistrées, il est impératif de respecter les conditions prescrites par l'article 73 de la loi organique numéro 63-2004 (dans le même sens que l'article 20 de la délibération de l'INPDP numéro 5 en date du 5 septembre 2018). L'article qui dispose qu'« Il est interdit de communiquer les enregistrements vidéo collectés à des fins de :

1. lorsque la personne concernée, ses héritiers ou son tuteur, ont donné leur consentement. Lorsque la personne concernée est un enfant, les dispositions de l'article 28 de la présente loi s'appliquent ;
2. lorsque la communication est nécessaire à l'exercice des missions dévolues aux autorités publiques ;
3. lorsque la communication s'avère nécessaire pour la constatation, la découverte ou la poursuite d'infractions pénales ».

La délibération dispose dans son article 21 qu' « En cas de remise d'une copie de l'enregistrement à la justice ou aux services de la police judiciaire ou dans le cadre de procédures disciplinaires internes, ce processus doit être inclus dans un dossier spécial conservé par le responsable du traitement qui est soumis au contrôle de l'instance ».

Si la communication a lieu à la demande de l'une des personnes ou autorités citées dans la loi et la délibération, le responsable de traitement est tenu de tenir un registre dans le quel il consigne les demandes d'accès aux enregistrements, l'identité de celui qui le demande, la date de la demande et de remise des enregistrements, le numéro de la caméra, l'heure et la date de l'enregistrement ainsi que sa durée et éventuellement les références de l'ordre judiciaire demandant la communication. Ce registre doit être tenu à la disposition de l'INPDP.

Si une personne demande d'accéder aux enregistrements où il est filmé ou qui peut servir à prouver ces droits ou une agression dont il a fait l'objet, le responsable de traitement ne doit pas s'exécuter mais demander à la personne concernée d'entamer une procédure judiciaire ou introduire une plainte qui permettras aux structures et autorités habiletés d'en faire la demande. Mais par contre, il doit faire copie des enregistrements sur un support externe pour éviter son effacement par le réglage automatique de l'enregistreur. Mention doit être portée au registre indiqué supra.

Dans tous les cas il est formellement interdit pour tout responsable de traitement de publier les vidéos collectées par exemple sur internet sans

le consentement explicite et laissant une trace écrite de la personne concernée.

X. Les développements récents

On recourt généralement à la vidéoprotection pour réaliser les finalités classiques qui ont été développées supra. Mais les technologies ont évolué en greffant dessus d'autres procédés intrusifs qui permettent non pas seulement d'enregistrer les images mais de les traiter pour des finalités spécifiques. C'est le cas de la reconnaissance faciale et celle des plaques d'immatriculation des voitures automobiles.

Les technologies récentes permettent à travers les enregistrements vidéo et en référence à une base de données de photos de procéder soit à l'authentification d'une personne pour vérifier que c'est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès) ou d'identifier une personne, donc de la retrouver dans les enregistrements.

Grâce au développement des technologies de traitement des données et de l'augmentation de la puissance de calcul des ordinateurs les deux opérations d'authentification ou d'identification deviennent possibles aujourd'hui en temps réel. L'opération sur le plan technique passe par la création d'un gabarit du visage analysé à travers ces caractéristiques, ce qui constitue un traitement de données biométriques qui sont des données sensibles.

Le cadre juridique tunisien attribue la mission d'autoriser ou pas le recours à ce procédé à l'INPDP qui doit recevoir dans ce cas deux demandes d'autorisation, l'une pour l'installation d'un système de vidéoprotection et la deuxième concernant le traitement des données biométriques. Il revient à l'Instance d'analyser la finalité du recours à ce procédé et de décider si le principe de proportionnalité a été ou pas respecté.

Ce cas de figure ne s'étant pas posé à l'INPDP, on peut présenter un cas en droit comparée. En Europe et dans le cadre du RGPD, il y a une interdiction de principe concernant la reconnaissance faciale sauf des cas exceptionnels. Ceux-ci sont prévus quand la personne a donné son consentement, si la reconnaissance a été rendu publique par la personne ou encore que cette opération est rendu nécessaire pour des motifs d'intérêt public (sécurité publique ou sureté de l'Etat). Dans tous les cas le règlement précise que le recours à l'identification biométrique ne peut être imposé à un individu et qu'il faut proposer à l'individu une mesure.

Le couplage d'enregistrement vidéo avec une plaque d'immatriculation est issu d'un système de lecture automatisée des plaques d'immatriculation des véhicules et qui permet d'analyser les flux vidéo issus de boîtiers de prise de vue afin de capturer et de lire en temps réel les plaques d'immatriculation des véhicules passant dans le champ des caméras de vidéoprotection.

Cette collecte massive de plaques d'immatriculation et de photographies des véhicules, sans justification particulière, constitue, par son caractère excessif, un manquement au principe de proportionnalité garanti par l'article 49 de la Constitution. En effet, un traitement ne peut porter que sur des données à caractère personnel adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

Dans ce cadre en 2019, des lycées en France se sont vus refuser le recours à ce procédé pour contrôler l'accès des lycéens à leur établissement. La CNIL avait rendu un avis négatif estimant que le dispositif était contraire aux grands principes de proportionnalité et de minimisation des données.

Quant au deuxième procédé, il est relatif loin de la biométrie de recourir à la reconnaissance automatique à travers les images de vidéoprotection, les plaques d'immatriculation des voitures automobiles.

Les finalités du recours à ce procédé peuvent être le contrôle d'accès à des espaces, la constatation d'infractions ou de crimes, la répression des actes de terrorisme ou de vandalisme ou encore la préservation de l'ordre public.

Dans tous ces cas, le procédé étant un traitement de données personnelles, il reste soumis préalablement à l'autorisation de l'INPDP car il passe par la vidéoprotection qui met à disposition les images et qui est un procédé soumis à l'autorisation de l'autorité de contrôle.

Ces procédés intrusifs qui touchent à la liberté de circulation et surtout de se déplacer de manière anonyme dans les espaces publics doivent répondre à des garanties de préservation des droits et libertés des individus. Le fondement reste l'article 49 de la constitution qui pose deux conditions essentielles, la nécessité et la proportionnalité de ces mesures.

On constate quotidiennement le recours à ce procédé par des intervenants privées et publics. Le parking de l'aéroport de Tunis Carthage recours à ce procédé. Le ticket porte le numéro d'immatriculation de la voiture. La justification est qu'il est ainsi impossible de faire sortir une voiture sans avoir le ticket identifié qui a été remis à l'entrée. C'est le cas aussi de certains hôtels pour l'accès à leur parking. Le ministre de l'intérieur a même annoncé à l'assemblée des représentants du peuple l'intention du ministère d'installer des caméras de surveillance dotées de ce procédé dans les entrées et sorties des grandes villes. Il est important de vérifier la sécurité de ces données ainsi que la durée de conservation des données et la qualité des personnes habilités à les consulter mais aussi l'existence ou pas d'un fichier de référence comprenant la base de données des plaques et de l'identité de leurs propriétaires.

XI. Plaintes et sanctions

Les normes mises en place et explicités doivent être respectés par les responsables de traitement. Toute violation des règles et des procédures peut entrainer l'introduction de plaintes de la part des personnes lésées qui peuvent entrainer l'application de peines assez lourdes.

XI. 1. Porter plainte

Si une personne considère que l'installation ou le traitement des données issues d'un système de vidéoprotection lui portent préjudice et viole sa vie privée et ses données personnelles, il peut porter plainte auprès de l'INPDP.

L'article 76 de la loi organique numéro 63-2004 attribue cette mission à l'Instance de « … recevoir les plaintes portées dans le cadre de la compétence qui lui est attribuée en vertu de la présente loi … ».

La plainte doit être rédigée sur papier libre. Un modèle indicatif est mis à la disposition des personnes intéressées en ligne à travers le lien www.inpdp.nat.tn/VS.pdf. Le modèle est en annexe de ce référentiel.

La plainte doit être accompagné d'une copie de la pièce d'identité du plaignant et indiquer les informations nécessaires pour que l'Instance puisse juger du bien-fondé de la plainte et surtout de la violation de la loi de 2004.

L'Instance n'ayant pas les moyens de constater les infractions, la plainte contre des installations illégales ou non conformes à une autorisation de l'Instance, doit être impérativement accompagnée par un constat d'huissier notaire avec photographies indiquant l'orientation et les espaces couverts par le champ des caméras installées.

Si l'Instance constate l'absence d'autorisation ou si l'installation a été réalisée en violation de l'autorisation qu'elle a donnée ou si les enregistrements ont été communiqués à des tiers ou diffusées en public, son Conseil prend la décision de transférer le dossier au Procureur de la République territorialement compétent.

L'article 77 de la loi organique numéro 63-2004 dispose que « … L'Instance doit informer le procureur de la République territorialement compétent de toutes les infractions dont elle a eu connaissance dans le cadre de son travail … ». Ainsi l'Instance ne fait que transférer le dossier, elle n'est ni plaignante, ni témoin, ni partie au procès. Il revient au Procureur de la République d'entamer s'il le juge nécessaire les procédures qui s'imposent.

Si suite à une plainte l'Instance décide de retirer une autorisation donnée au responsable de traitement qui ne l'a pas respecté, la procédure est régie par

le chapitre IV du décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel.

Le décret arrête la procédure à suivre dans les articles 13 et 14. Celle-ci est la suivante :

- Le responsable de traitement est convoqué par lettre recommandée avec accusé de réception ou tout autre moyen laissant une trace écrite pour son audition à l'Instance au moins sept jours avant ;
- Après l'audition l'Instance peut décider :
  - soit de lui donner la possibilité de se conformer aux normes légales ;
  - soit de lui retirer l'autorisation ;
- Si la violation est clairement établie, l'Instance peut interdire le traitement de manière provisoire pour un délai ne dépassant pas un mois en attendant la prise de la décision définitive

La procédure du recours devant l'instance et de la procédure et des suites à lui donner sont explicités par l'article 24 de la délibération numéro 5 en date du 5 septembre 2018.

XI. 2. Les sanctions encourues

La violation des normes légales relatives à l'installation des systèmes de vidéoprotection ainsi que du traitement des données enregistrées sont sanctionnées par un chapitre VII de la loi organique numéro 63-2004.

Les sanctions prévues par le législateur sont très dissuasives car elles portent sur des peines privatives de liberté en plus des amendes.

Ces peines prononcées par le juge pénal sont appliquées au responsable de traitement fautif directement si c'est une personne physique et « lorsque le contrevenant est une personne morale, les peines prévues ci-dessus sont applicable personnellement et selon les cas au dirigeant légal ou de fait de la personne morale dont la responsabilité concernant les actes accomplis a été établie » (article 101).

Les articles concernant la vidéoprotection portent les numéros de 69 à 74. Les violations de ces dispositions se retrouvent dans les dispositions de la section réservée aux sanctions :

Article 87. Est puni d'un emprisonnement de deux ans et d'une amende de dix mille dinars, celui qui viole les dispositions de … articles 70 et 71 de la présente loi

Article 89. Est puni d'un an d'emprisonnement et d'une amende de cinq mille dinars, celui qui intentionnellement communique des données à caractère personnel pour réaliser un profit pour son compte personnel ou le compte d'autrui ou pour causer un préjudice à la personne concernée

Article 90. Est puni d'un an d'emprisonnement et d'une amende de cinq mille dinars, quiconque :

- effectue intentionnellement un traitement des données à caractère personnel … sans l'obtention de l'autorisation prévue aux articles 15 et 69 de la présente loi, ou continue d'effectuer le traitement des données après l'interdiction de traitement ou le retrait de l'autorisation

- communique les données à caractère personnel sans le consentement de la personne concernée ou l'accord de l'Instance dans les cas prévus par la présente loi

Article 93. Est puni de trois mois d'emprisonnement et d'une amende de trois mille dinars quiconque diffuse intentionnellement des données à caractère personnel, à l'occasion de leur traitement, d'une manière qui nuit à la personne concernée ou à sa vie privée.

La peine est d'un mois d'emprisonnement et d'une amende de mille dinars lorsque la diffusion a été effectuée sans l'intention de nuire

Article 94. Est puni de trois mois d'emprisonnement et d'une amende de mille dinars quiconque viole les dispositions des articles … 74 de la présente loi.

Est puni également des mêmes peines prévues au paragraphe précédent quiconque collecte des données à caractère personnel à des fins illégitimes ou contraires à l'ordre public ou traite intentionnellement des données à caractère personnel inexactes, non mises à jour ou qui ne sont pas nécessaires à l'activité de traitement.

ANNEXES

1، نهج محمد معلى، مينوال فيل، 1002، تونس من.ب. 525
الهاتف (+216) 71 799 853 - 71 799 711 الفاكس 71 799 823
1, Rue Mohamed Moalla, 1002, Tunis, Tunisie B.P. 525
Tél. (+216) 71 799 853 - 71 799 711 Fax 71 799 823
inpdp@inpdp.tn www.inpdp.tn

INPDP
الهيئة الوطنية لحماية المعطيات الشخصية
INSTANCE NATIONALE DE PROTECTION DES DONNEES PERSONNELLES
NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

مطلب ترخيص مسبق لتركيز وسائل مراقبة بصرية

DEMANDE D'AUTORISATION PRÉALABLE D'INSTALLATION D'UN SYSTÈME DE VIDÉOSURVEILLANCE

الفصل 10 من الأمر عدد 3004-2007 بتاريخ 27 نوفمبر 2007 — الفصول 69 الى 74 من القانون الأساسي عدد 63-2004 بتاريخ 27 جويلية 2004

Article 10 du décret n° 2007-3004 du 27 novembre 2007 — Articles 69 à 74 de la loi organique n° 63 2004-du 27 juillet 2004

يرفق وجوبا هذا المطلب بالمثال الهندسي يشخص أماكن ووجهة وسائل المراقبة البصرية
La demande doit impérativement comporter un plan général d'installation des caméras de surveillance et de leur champ de vision ainsi que des images des caméras ou avant installation d'un appareil photo avec la même orientation que les caméras qui seront installés

1. Demande (Réservé à l'INPDP) — 1. المطلب (خاص بالهيئة)

Date — التاريخ

Moyen — الوسيلة — Papier ☐ ورقية — Electronique ☐ الكترونية — Postale ☐ بريد

Référence enregistrement — مرجع تسجيل التصريح

2. Demandeur — 2. الطالب

Nature — الطبيعة — Physique ☐ طبيعي — Pers. Pub. ☐ شخص عمومي — Société ☐ شركة — Association ☐ جمعية — Parti ☐ حزب

Identité — الهوية

Adresse — العنوان

Code postal — الترقيم البريدي — **Ville** — المدينة

Tél. fixe — الهاتف القار — **Tél. portable** — الهاتف الجوال

Adresse électronique — العنوان الالكتروني — @

Personne contact — الشخص المعني

G.S.M. — الجوال — **E-mail** — العنوان الالكتروني — @

3. Finalité de l'installation — 3. الغرض من تركيز الوسائل

Sécurité des personnes	☐	حماية الأشخاص
Protection des bâtiments	☐	حماية الممتلكات
Prévention des fraudes et vols	☐	الوقاية من التحيل والسرقة
Prévention des risques	☐	الوقاية من الحوادث
Régulation du flux	☐	تنظيم حركة التنقل
Prévention des atteintes aux biens	☐	حماية التجهيزات
Autres, spécifiez	☐	أخرى، أذكرها

4. Localisation du système — 4. موقع تركيز نظام المراقبة

Adresse — العنوان

Code postal — الترقيم البريدي — Ville — المدينة

Coordonnées GPS — العنوان GPS

Latitude — خط العرض — Longitude — خط الطول

5. Nombre & type de caméras — 5. عدد ومواصفات آلات المراقبة

Caméras fixes — عدد الآلات القارة — Caméras mobiles — عدد الآلات المتحركة

Caméras intérieures — عدد الآلات الداخلية — Caméras extérieures — عدد الآلات الخارجية

Nombre de jours de conservation des vidéos — عدد أيام حفظ التسجيلات الفيديو

Retransmission en direct des images — Oui ☐ نعم — Non ☐ لا — وجود نظام بث حيني للصور

Retransmission en différé des images — Oui ☐ نعم — Non ☐ لا — وجود نظام بث غير مباشر للصور

6. Installateur du système — 6. الطرف المركز لوسائل المراقبة

Identité et coordonnées de l'installateur — هوية وعنوان الشركة التي ركزت نظام المراقبة

Identité — الهوية

Adresse — العنوان

Code postal — الترقيم البريدي — Ville — المدينة

Tél. fixe — الهاتف القار — Tél. portable — الهاتف الجوال

Adresse électronique — @ — العنوان الالكتروني

7. Personnes habilitées à y accéder — 7. الأشخاص المخول لهم الاطلاع

Nom — الاسم — Prénom — اللقب — Fonction — الوظيفة

Nom — الاسم — Prénom — اللقب — Fonction — الوظيفة

Nom — الاسم — Prénom — اللقب — Fonction — الوظيفة

Nom — الاسم — Prénom — اللقب — Fonction — الوظيفة

8. Traitement des images — 8. معالجة التسجيلات

Les images sont traitées par le demandeur ? — Oui ☐ نعم — Non ☐ لا — يتم معالجة التسجيلات من طرف الطالب ؟

Autrement, à quelle adresse ? — اذا لا، ما هو موقع المعالجة ؟

Adresse — العنوان

Code postal — الترقيم البريدي — Ville — المدينة

9. Sécurité et confidentialité des données — 9. سلامة وسرية المعلومات

Quelles sont les mesures prises pour contrôler l'accès ? — ما هي الإجراءات المتبعة لمراقبة الولوج ؟

- Code d'accès ☐ شفرة ولوج
- Porte blindée ☐ باب مصفح
- Local surveillé ☐ محل مراقب
- Local fermé à clé ☐ محل مغلق بمفتاح

Quelles sont les mesures prises pour la sauvegarde ? — ما هي الإجراءات المتبعة لحفظ التسجيلات ؟

Quelles sont les mesures prises pour la destruction ? — ما هي الإجراءات المتبعة لإعدام التسجيلات ؟

10. Information du public — 10. إجراءات اعلام العموم

Indiquez le nombre d'affiches d'information — أذكر عدد معلقات الاعلام

Précisez la localisation de l'affichage — أذكر أماكن التعليق

11. Exercice du droit d'accès — 11. ممارسة حق النفاذ

Personne contact — الشخص المعني

Adresse — العنوان

Code postal — الترقيم البريدي — Ville — المدينة

Tél. fixe — الهاتف القار — Tél. portable — الهاتف الجوال

Adresse électronique — @ — العنوان الالكتروني

12. Engagement et déclaration sur l'honneur — 12. التزام و تصريح على الشرف

اني الممضي اسفله،

- التزم بمعالجة المعطيات الشخصية موضوع التصريح وفق المقتضيات الواجبة قانونا والمحددة بالقانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004 والنصوص التطبيقية المتعلقة بحماية المعطيات الشخصية في تونس.
- كما التزم بإعلام الهيئة عند وقوع أي تغيير في المعلومات المدلى بها في هذا التصريح.
- وأصرح بأني على علم بأن هذه المعطيات سيتم معالجتها في إطار قاعدة بيانات تكون متاحة للعموم على موقع الهيئة.
- أصرح على الشرف باحترام الشروط القانونية للمعالجة وخاصة منها التمتع بالجنسية التونسية للمصرح والمعالج للمعطيات الشخصية، نقي السوابق العدلية ومقيم بالبلاد التونسية.

Je soussigné,

- M'engage à traiter les données personnelles, objet de cette déclaration, conformément aux règles juridiques de protection des données personnelles telles que fixées par la loi organique numéro 63 de 2004 en date du 27 juillet 2004 ainsi que les textes d'application relatifs à la protection des données personnelles en Tunisie.
- M'engage aussi à informer l'instance de chaque modification qui survient sur les données déclarées.
- Déclare avoir été mis au courant du traitement de ces données dans une base de donnée qui sera ouverte à consultation sur le site de l'instance.
- Je déclare sur l'honneur la conformité du traitement aux obligations légales et notamment : La nationalité tunisienne des responsables du traitement et de leurs sous-traitants, l'absence d'antécédents judiciaires.

Nom & prénom & qualité — الاسم واللقب والصفة

Date et lieu — التاريخ و المكان

طبقا لمقتضيات القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004 تتمتعون بحق النفاذ الى المعطيات التي تخصكم وطلب تحيينها
وبمكنكم ممارسة هذا الحق بمقر الهيئة بالعنوان : 1، نهج محمد معلي، ميتوال فيل، تونس
او عن طريق البريد الالكتروني : acces [at] inpdp.tn

Conformément à la loi organique numéro 63-2004 du 27 juillet 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent,
Vous pouvez exercer ce droit au siège de l'instance à l'adresse : 1, rue Mohamed Moalla, Mutuelle ville, Tunis
ou par mail à l'adresse acces [at] inpdp.tn

الهيئة الوطنية لحماية المعطيات الشخصية
INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES
NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

شكاية حول خرق قواعد تركيز وسائل مراقبة بصرية

إني الممضي على هذا، ..... صاحب بطاقة التعريف الوطنية (أو جواز سفر بالنسبة لغير التونسيين) رقم ..... الصادر بتاريخ..... أتقدم إلى الهيئة الوطنية لحماية المعطيات الشخصية بهذه الشكوى ضد ..... بصفته مسؤول على معالجة معطيات شخصية عبر تركيز وسائل مراقبة بصرية بالأماكن التالية .....
..... بالعنوان التالي .....

.....

علما وأن هذه الأفعال تشكل خرقا للفصول 69 و70 من القانون الأساسي عدد 63 المؤرخ 27 جويلية 2004 وتنطبق عليها العقوبات الواردة بالفصول 87 و90 من نفس القانون.

وبناء عليه وعملا بمقتضيات الفصلين 76 و77 من القانون المذكور أطلب من الهيئة إجراء التحقيقات اللازمة ومعاينة الجريمة وإعلام وكيل الجمهورية المختص ترابيا قصد إجراء ما يتعين.

هذا وإني أحتفظ بحقي في القيام بالحق الشخصي في طلب جبر الأضرار التي لحقتني من جراء هذه الأفعال المجرمة.

أرفق بهذه الشكوى معاينة عن طريق عدل منفذ لتواجد هذه الوسائل مع صور شمسية مبينة لذلك.