REPUBLIQUE ET CANTON DE GENEVE
Département en charge de la Police
Police

ORGANISATION ET USAGE DE LA VIDÉOSURVEILLANCE	
Type : Directive de service	**No** : DS OSI.02.01
Domaine : Organisation et sécurité de l'information	
Rédaction : M. Realini - S. Gisler	**Validation** : M. Bonfanti
Entrée en vigueur : 13.10.2014	**Mise à jour** : 19.10.2022

Objectif(s)

Cette directive a pour objectifs d'organiser et de fixer le cadre légal ainsi que la procédure relative à l'usage de la vidéosurveillance par la police.

Champ d'application

- Ensemble des directions et services de la police.

Documents de référence

- Code de procédure pénale suisse (ci-après : CPP) RS 312.0.
- Code des obligations (ci-après : CO) RS 220.0.
- Code pénal suisse (ci-après : CP) RS 311.0.
- Concordat sur les entreprises de sécurité (CES) RSG I 2 14.
- Constitution fédérale de la Confédération suisse (Cst) RS 101.
- Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) RS 0.101.
- Convention européenne sur la violence et les débordements de spectateurs lors de manifestations sportives et notamment de matches de football RS 0.415.3.
- Loi fédérale sur l'aide aux victimes d'infractions (ci-après : LAVI) RS 312.5.
- Loi fédérale sur la protection des données (ci-après : LPD) RS 235.1.
- Loi sur la police (ci-après : LPol) RSG F 1 05.
- Loi sur les manifestations sur le domaine public (ci-après : LMDPu) RSG F 3 10.
- Loi sur les renseignements et les dossiers de police et la délivrance des certificats de bonne vie et mœurs (LCBVM) RSG F 1 25.
- Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (ci-après : LIPAD) RSG A 2 08.
- Ordonnance 3 relative à la loi sur le travail (ci-après : OLT 3) RS 822.113.
- Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (ci-après : RIPAD) RSG A 2 08.01.
- Règlement sur l'organisation de la police (ci-après : ROPol) RSG F 1 05.01.
- Règlement sur l'organisation et la gouvernance des systèmes d'information et de communication (ROGSIC) RSG B 4 23.03.

Directives de police liées

- Prescriptions en matière de vidéosurveillance exercée par des privés, DS OSI.02.17.
- Prises de vues lors de manifestations, OS PRS.02.05.
- Privilèges et immunités diplomatiques, OS PRS.11.01.

Autorités et fonctions citées

- Chef des opérations (ci-après : chef OP).
- Chef d'état-major (ci-après : chef EM).
- Chef du centre de compétences des systèmes d'information police (ci-après : chef du CCSIP).

- Chef du centre des opérations et de la planification (ci-après : chef COP).
- Chef du département en charge de la police (ci-après : chef du Département).
- Commandant de la police (ci-après : CDT).
- Commissaire de police de service (ci-après : COMS).
- Officier chargé de la vidéosurveillance.
- Préposé cantonal à la protection des données et à la transparence (ci-après : PPDT).
- Procureur général (ci-après : PG).

Entités citées et abréviations

- Agent de police municipale (ci-après : APM).
- "Automatisiertes Büro Infomationsystem" - Données genevoises des personnes et des affaires (ci-après : myABI).
- Brigade judiciaire aéroport (ci-après : BAERO).
- Brigade sécurité diplomatique (ci-après : BSD).
- Centrale d'engagement, de coordination et d'alarme (ci-après : CECAL).
- Centrale des opérations de la police internationale (ci-après : COPI).
- Centrale de surveillance et d'intervention (ci-après : CSI).
- Centrale de vidéoprotection (ci-après : CVP).
- Centre de compétences des systèmes d'information police (ci-après : CCSIP).
- Chemins de fer fédéraux (ci-après : CFF).
- Direction des finances police (ci-après : DFP).
- Département en charge de la police.
- Département en charge de l'instruction.
- Direction de la stratégie (ci-après : DSTRAT).
- Enquêteur de sécurité publique (ci-après : ESP).
- État-major Police (ci-après : EMP).
- Fondation des parkings.
- Genève-Aéroport.
- Groupe technique de recherches de véhicules (GTRV).
- Inspection générale des services (ci-après : IGS).
- Ministère public (ci-après : MP).
- Mission suisse.
- Nouvel hôtel de Police (ci-après : NHP).
- Office cantonal des systèmes d'information et du numérique (ci-après : OCSIN).
- Office cantonal des transports (ci-après : OCT).
- Office fédéral de la douane et de la sécurité des frontières (ci-après : OFDF).
- Office fédéral des routes (ci-après : OFROU).
- Poste de commandement Police (ci-après : PCP).
- Poste suisse (ci-après : la Poste).
- SBB Transportpolizei - Police des transports CFF (ci-après : TPO).
- Secteur de la sécurité de l'information (ci-après : SSI).
- Service des contraventions (ci-après : SDC).
- Transports publics genevois (ci-après : TPG).
- Tribunal des mineurs (ci-après : TMin).

Mots-clés

- Accès aux données.
- Caméra.
- "Cyclope".
- Données personnelles.
- Eagle.

- Espace public.
- Extraction d'image.
- Images.
- Ordre de dépôt.
- Pièce à conviction.
- Preuve.
- Remboursement.
- Surveillance.
- Vidéoprotection.
- Vidéosurveillance.

Annexes

- Annexe 1 : autorités de validation des extractions.
- Annexe 2 : intervenants et rôles "Cyclope".
- Annexe 3 : intervenants et rôle CVP.
- Annexe 4 : procédure d'extraction d'images ou de séquence vidéo.

1. PRÉAMBULE

Au sens de la présente, la vidéosurveillance est un système de caméras permettant l'acquisition, le stockage et la diffusion d'images, disposées dans le domaine public ou privé.

Elle vise à en assurer la sécurité et contribue à l'accomplissement des missions, ainsi qu'à l'établissement des infractions commises et l'identification de leurs auteurs.

La vidéosurveillance peut comprendre :

- le visionnement et le traitement d'images obtenues au moyen de caméras :
  - de l'administration cantonale, des administrations communales et des institutions de droit public du canton de Genève;
  - des services de l'administration fédérale et des sociétés anonymes de droit public;
  - des privés;
  - du milieu diplomatique;
- l'exploitation par la police de ses propres systèmes de vidéosurveillance, le visionnement et le traitement d'images obtenues au moyen de ses caméras.

La présente directive s'articule autour de :

- l'acquisition des images de vidéosurveillance;
- la diffusion des images;
- le traitement et le stockage des images.

2. GÉNÉRALITÉS

2.1. Définitions

Dans la présente directive, on entend par :

- champ de vision : zone de couverture de la caméra et le degré de détail pouvant être visualisé;
- communication : le fait de rendre accessibles des données ou un document en autorisant leur consultation, en les transmettant ou en diffusant des copies;
- données personnelles (ou données) : toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable;
- enregistrement des images : moyen technique permettant de fixer, de conserver et de reproduire des images;
- exploitation de systèmes de vidéosurveillance : installation et mise en service d'un système de vidéosurveillance et traitement des données collectées;
- extraction : procédure visant à obtenir la délivrance d'images ou de séquences de vidéosurveillance, au-delà du délai de conservation automatique;
- marquage ou préservation : procédure visant à obtenir la préservation d'images ou de séquences de vidéosurveillance, au-delà du délai de conservation automatique;
- traitement des données : toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données;
- vidéosurveillance "Cyclope" : système de vidéosurveillance de la police dédié aux évènements majeurs et au milieu diplomatique.

2.2. Bases légales

La vidéosurveillance est réglée de manière générale aux articles 42 LIPAD et 16 RIPAD et de manière spécifique dans les lois spéciales suivantes :

- l'article 6 LMDPu, dans le cadre des manifestations sur le domaine public;
- les articles 282 et suivants CPP, s'agissant de l'activité de police judiciaire ou lorsqu'elle est utilisée dans le cadre d'une procédure pénale;
- les articles 61 LPol et 18 à 20 ROPol, s'agissant de l'activité de la police dans son ensemble.

La captation de son est proscrite, n'étant fondée à l'heure actuelle sur aucune base légale. Les microphones des dispositifs qui en sont équipés sont désactivés.

3. ACQUISITION D'IMAGES

3.1. Généralités

3.1.1. Proportionnalité

L'utilisation de la vidéosurveillance doit être proportionnelle, c'est-à-dire être propre et nécessaire à garantir la sécurité des personnes et des biens se trouvant dans ou à proximité immédiate de lieux publics ou affectés à l'activité d'institutions publiques, en prévenant la commission d'agressions ou de déprédations et en contribuant à l'établissement des infractions commises le cas échéant (article 42 LIPAD).

Dès lors, le champ de vision des caméras est limité au périmètre nécessaire à l'accomplissement de la surveillance.

Lorsque la surveillance, en particulier le champ de vision des caméras, risque de constituer une atteinte excessive à la sphère privée, il est procédé à la dissimulation des zones litigieuses, au moyen de techniques physiques ou informatiques appropriées (masquage, floutage, pixellisation), à moins qu'un intérêt public prépondérant ne s'y oppose.

3.1.2. Signalétique

La police et ses partenaires techniques (notamment l'OCSIN) s'assurent que l'existence d'un système de vidéosurveillance est signalée de manière adéquate au public et au personnel de la police.

Une signalétique est apposée dans le périmètre sous vidéosurveillance, de manière visible, pour informer les personnes filmées.

3.2. Voie publique

3.2.1. Interdiction de filmer devant un établissement scolaire

Hors d'une procédure pénale, la police s'assure de ne pas filmer un établissement scolaire ou ses abords immédiats durant les heures des activités scolaires et parascolaires, sauf autorisation expresse ou demande du Département en charge de l'instruction publique (article 16 alinéa 7 RIPAD).

3.2.2. Lors de manifestations sur le domaine public

La police peut filmer les participants à une manifestation s'il ressort des circonstances concrètes que certaines de ces personnes envisagent de commettre un crime ou un délit dont la gravité ou la particularité justifie cette mesure (article 6 alinéa 5 LMDPu).

La vidéosurveillance exercée à cette occasion est soumise aux conditions générales prévues par la présente directive et aux conditions spécifiques de l'OS PRS.02.05.

3.3. Locaux de police

3.3.1. Locaux et zones accessibles au public

Selon l'article 61 alinéa 1 LPol, les postes de police et les locaux de la police judiciaire sont équipés de caméras.

La vidéosurveillance est déployée dans les lieux auxquels les justiciables ont accès, dans lesquels ils peuvent être retenus, interrogés et soumis aux diverses opérations d'enquête qui découlent de l'accomplissement des missions de la police.

Les locaux concernés sont les suivants :

- couloirs et escaliers accessibles au public ou aux prévenus;
- salles d'audition;
- salles LAVI;
- violons (sauf partie toilettes);
- zones accessibles au public (avant-poste, accueil, guichet);
- zones de rétentions.

Sont également concernées les zones suivantes :

- accès aux bâtiments (points d'entrée);
- périmètre des bâtiments;
- zones de chargement et de déchargement de personnes;
- zones de stationnement des véhicules de police.

Ces installations permettent de disposer d'éléments de preuve en cas de survenance d'incidents, de doléances, de plaintes ou de dénonciations pouvant déboucher sur une procédure pénale ou administrative impliquant un membre du personnel de la police.

Des caméras de vidéosurveillance sont également installées à l'extérieur des bâtiments dans le but de protéger les locaux, véhicules et infrastructures de la police contre des déprédations.

3.3.2. Mesures spécifiques

La vidéosurveillance ne doit pas constituer une atteinte à la sphère privée ou au secret professionnel. A ce titre, le dispositif de vidéosurveillance peut être désactivé :

- dans les violons, si le détenu s'y trouve seul;
- lors de la fouille ou d'examens médicaux;
- lors d'entretiens du prévenu avec son avocat, sauf requête contraire de ce dernier.

3.3.3. Protection du personnel

L'utilisation de la vidéosurveillance aux fins de contrôle des activités du personnel est proscrite (article 19 alinéas 2 et 3 ROPol).

Les locaux utilisés uniquement par les membres du personnel ne peuvent être filmés conformément à la législation y relative (article 328 CO et 26 alinéa 1er OLT 3).

Les locaux concernés sont les suivants :

- couloirs et escaliers non accessibles au public;
- espaces de travail personnel, bureaux;
- local de pause;
- local des pièces à conviction ou des objets trouvés;
- salles d'armes;
- vestiaires.

Des dispositions sont prises afin que, le personnel ne se trouve pas de manière permanente et directe dans le champ de vision des caméras.

S'il n'est pas possible de respecter cette exigence, un procédé technique est utilisé pour rendre non identifiables les membres du personnel (article 42 alinéa 1er lettre d LIPAD).

3.4. Utilisation par la police de caméras de tiers

3.4.1. Principe

La police peut, dans le cadre de l'interconnexion entre systèmes de vidéosurveillance, être autorisée à accéder à tous les systèmes de vidéosurveillance des institutions publiques, que ceux-ci filment ou non le domaine public.

La police est autorisée à traiter des données enregistrées par des caméras de tierces personnes physiques ou morales de droit public ou de droit privé lorsque ces données sont utiles à la prévention ou à la poursuite d'un crime ou d'un délit (cf. DS OSI.02.17).

Elle peut traiter ces données dans le cadre d'évènements entrant dans son champ de mission. Dans tous les cas, lorsqu'une procédure pénale est en cours, les dispositions du CPP sont applicables.

3.4.2. Tiers exploitant des caméras

3.4.2.1. Caméras d'institutions publiques

Il s'agit des systèmes de vidéosurveillance installés par l'administration cantonale, les administrations communales et les institutions de droit public du canton de Genève.

Cette vidéosurveillance est soumise aux lois cantonales et en particulier à la LIPAD et au RIPAD.

A teneur de l'article 16 alinéa 5 RIPAD, les institutions publiques sont tenues d'annoncer à la police tout système de vidéosurveillance dont le champ de surveillance porte sur le domaine public.

3.4.2.2. Caméras des services de l'administration fédérale et des sociétés anonymes de droit public

Ces caméras sont soumises au droit fédéral et notamment à la LPD (OFROU, CFF, TPO, la Poste et Genève-Aéroport).

3.4.2.3. Caméras exploitées par des personnes physiques ou morales de droit privé

Cette vidéosurveillance est régie par les dispositions de la LPD.

Celle-ci doit porter sur un espace privé et avoir pour finalité la défense d'un intérêt prépondérant comme la protection des biens ou des personnes (cf. DS OSI.02.17).

3.4.2.4. Caméras en lien avec le milieu diplomatique

Plusieurs organisations internationales et représentations diplomatiques ont leur siège ou sont présentes à Genève en vertu de dispositions légales ou d'accords conclus avec la Confédération.

Ces entités exploitent des systèmes de vidéosurveillance et sont soumises à des dispositions légales qui leur sont propres (cf. OS PRS.11.01).

Il convient de s'adresser à la BSD pour toute demande relative à des images de vidéosurveillance provenant de caméras installées par les missions permanentes et les organisations internationales.

La BSD se charge de faire la demande d'extraction via la Mission suisse.

S'agissant des images provenant de caméras sur la voie publique qui filment les organisations internationales et les représentations diplomatiques, il faut s'adresser à la COPI.

3.4.3. Accès par délégation

La police peut être délégataire de l'exploitation d'un système de vidéosurveillance appartenant à une institution publique lorsque, cumulativement :

- cette délégation a été approuvée préalablement par les instances dirigeantes de l'institution publique responsable;
- le système de vidéosurveillance concerné satisfait aux exigences de l'article 42 LIPAD et à celles de l'article 16 RIPAD;
- l'institution publique ne dispose pas du personnel qualifié pour en assurer l'exploitation alors que le système de vidéosurveillance est indispensable à la prévention d'agressions ou de déprédations;
- une convention expressément conclue avec l'institution publique et signée par le chef du Département, le prévoit.

4. TRAITEMENT ET STOCKAGE

4.1. Principes

Les images de vidéosurveillance doivent être traitées et stockées afin de permettre leur consultation et leur conservation conformément aux dispositions légales et notamment quant à leur durée (cf. point 4.2.).

4.1.1. CVP

La CVP est l'entité responsable de la gestion opérationnelle des images de vidéosurveillance recueillies sur le domaine public, ainsi que dans les locaux de police.

Ses missions sont notamment à travers l'usage de la vidéosurveillance :

- d'assister les policiers dans leur engagement;
- de participer à la prévention de la commission d'infractions;
- de procéder à des mesures d'investigation relatives à des évènements se déroulant sur le domaine public;
- de procéder à la recherche de personnes sur la base de signalements.

Par ailleurs, la CVP s'assure de la disponibilité et du blocage des images de vidéosurveillance sur demande ou de sa propre initiative.

La CVP apporte un soutien logistique dans l'acquisition, le traitement et la diffusion des images aux policiers.

Pour des raisons de confidentialité, l'accès aux locaux de la CVP est strictement limité aux collaborateurs expressément autorisés.

En vue d'assurer la traçabilité des accès physiques, les noms, prénoms et matricules de toutes les personnes accédant à ces locaux sont consignés dans un registre. Les dates et heures d'entrée et de sortie des locaux y sont également mentionnées.

Des mesures techniques de contrôle des accès peuvent être mises en œuvre.

4.1.2. CCSIP

Le CCSIP et le SSI sont les entités responsables, dans la limite de leurs compétences respectives, de la sécurité des données obtenues au moyen de la vidéosurveillance. Les aspects relevant de l'OCSIN demeurent réservés.

Hors enquête ou procédure judiciaire, le visionnement des données, enregistrées ou non, issues de la vidéosurveillance est strictement limité à un cercle restreint de personnes dûment autorisées pour un but uniquement technique. La liste de ces personnes est dressée et conservée par le chef du CCSIP ou la personne désignée par lui-même (article 13 alinéa 3 RIPAD).

Le chef du CCSIP s'assure que cette liste reste à jour et veille à ce que le CDT, le chef EM et le PPDT en possèdent une copie.

4.1.3. SSI

En collaboration avec les services compétents, le SSI organise, au minimum une fois tous les deux ans à compter de leur mise en service, une vérification de la sécurité et de la conformité technique de toutes les installations de vidéosurveillance appartenant à la police ou dont la gestion lui est déléguée (orientation, état de fonctionnement, sécurité physique des caméras, signalétique, etc.).

A cette occasion, il est procédé à l'analyse de toutes les interventions effectuées sur les installations depuis la date de la dernière vérification.

4.1.4. Officier chargé de la vidéosurveillance

Le chef EM fait fonction d'officier chargé de la vidéosurveillance.

Le chef EM tient, sous clé, un registre daté des enregistrements sauvegardés, toutes catégories confondues, ainsi que des visionnements effectués et des personnes concernées. Il rend compte mensuellement au CDT.

Les enregistrements sont cotés et mention en est faite dans le rapport afférent à l'incident.

4.1.5. Exploitation des images police

4.1.5.1. Préservation des images

La demande de préservation des images est systématique dans les cas suivants :

- lors de rixes, de violences ou de toute autre situation analogue qui le requiert;
- lors d'évasions;
- lors d'usage de la force par le personnel de la police, notamment avant ou durant un placement en cellule;
- lorsqu'une allégation de mauvais traitement parvient à sa connaissance, notamment sous la forme d'un constat de lésions traumatiques ou d'un signalement par le lésé, par un membre du personnel de la police ou par un tiers;
- lorsqu'un membre du personnel de la police est victime de violences;
- sur requête du MP, de l'IGS, du TMin ou du SDC.

Toute demande de préservation est validée par le chef du service concerné.

4.1.5.2. Extraction des images

Afin de pouvoir visionner les images, il faut au préalable faire une demande d'extraction.
Cette demande doit être validée par le chef EM, le COMS, le Chef OP, le chef COP ou l'IGS (cf annexe 1).

4.1.5.3. Visionnement des séquences vidéo

Le CDT ou un membre de l'état-major, qu'il désigne, peuvent procéder au visionnement des images extraites. Ils décident en outre des suites à donner.

En cas de procédure pénale, seuls le MP, l'IGS, le TMin et le SDC sont compétents pour le visionnage des images.

4.1.6. Exploitation des images tierces

L'exploitation des images de caméras appartenant à des entités tierces, est réglée par le CPP ou d'autre conventions spécifiques (voir chapitres 3.4. et 5.).

4.2. Délais de conservation des images

4.2.1. Voie publique

4.2.1.1. Délai ordinaire

Délai : 7 jours.

Les données enregistrées au moyen d'un système de vidéosurveillance doivent, en principe, être détruites dans un délai de 7 jours.

4.2.1.2. Délai lors d'atteinte avérée aux personnes et aux biens

Délai : 3 mois.

Le délai ordinaire de 7 jours est porté à 3 mois en cas d'atteinte avérée aux personnes ou aux biens (article 42 alinéa 2 LIPAD).

Dans cette hypothèse, la prolongation du délai de conservation se fait par le marquage de la séquence, comme décrit au chapitre 5.5.

Si aucune action n'est effectuée dans l'intervalle, cette sauvegarde sera détruite après une durée de 3 mois.

4.2.1.3. Délai lors de manifestation avec risques concrets

Délai : 30 jours.

Les données enregistrées par la police lors d'une manifestation sur l'espace public en application de l'article 6 LMDPu sont conservées pendant 30 jours après la manifestation.

Si celles-ci sont directement utiles à la poursuite d'un crime ou d'un délit survenu pendant la manifestation, elles seront conservées au-delà du délai de 30 jours sur autorisation du chef COP (article 6 alinéa 6 LMDPu).

4.2.2. Dans les locaux de la police

Délai ordinaire : 100 jours.

Les images filmées dans les postes de police, les locaux de la police judiciaire et les zones énumérées au point 3.3.1. sont conservées durant 100 jours, selon la teneur de l'article 61 LPol, avant d'être détruites, sauf décision émanant d'une autorité compétente par laquelle ce délai est prolongé.

4.2.3. Procédure pénale

Délai : jusqu'à l'issue de la procédure.

Lorsque les images sont utilisées dans le cadre d'une procédure pénale, elles sont conservées jusqu'à l'issue de cette dernière.

Lesdites images sont en outre remises d'office à l'autorité de poursuite pénale compétente par l'enquêteur en charge de l'affaire.

4.2.4. Utilisation des enregistrements à des fins de formation

A l'expiration des délais de conservation prévus ci-dessus, l'autorité de validation compétente (cf. annexe 1) peut autoriser la conservation de séquences vidéo et d'images obtenues au moyen des systèmes de vidéosurveillance de la police en vue de les utiliser dans le cadre de la formation.

Lorsque l'autorité de validation compétente (cf. annexe 1) l'estime nécessaire ou à la demande de l'autorité de poursuite pénale compétente, des procédés techniques d'anonymisation et/ou de floutage d'images et/ou de données personnelles (floutage de plaques d'immatriculation par exemple) sont appliqués pour cacher ces données et rendre non identifiables les personnes dont l'apparition sur les images ne serait pas justifiée.

4.3. Contrôle et suivi

4.3.1. Registre des activités techniques

Toutes les actions effectuées sur le système de vidéosurveillance sont répertoriées dans le registre des activités à des fins d'enquête et d'audit. Les registres ne sont en principe accessibles qu'au SSI et à l'IGS.

Le SSI rend un rapport de son activité au chef EM une fois par année ainsi qu'à chaque fois que les circonstances le commandent.

4.3.2. Audit de conformité

A la demande du chef EM, le SSI procède ou fait procéder à des contrôles afin de vérifier la conformité aux dispositions légales et réglementaires de l'utilisation des données issues de la vidéosurveillance.

4.3.3. Inventaire et cartographie des systèmes de vidéosurveillance

Dans le cadre de l'inventaire et de la cartographie des systèmes de vidéosurveillance installés par les institutions publiques et dont le champ de surveillance porte sur le domaine public, la DSTRAT reçoit les annonces d'installation de système de vidéosurveillance faites par les institutions concernées, en application de l'article 16 alinéa 5 RIPAD.

La DSTRAT s'assure que les formulaires d'annonce mentionnent pour chaque dispositif de vidéosurveillance installé :

- la finalité de la vidéosurveillance;
- le cercle et le statut des personnes autorisées à visionner les images;

- l'enregistrement ou non des images et leur durée de conservation;
- les zones placées sous vidéosurveillance;
- le type de visionnement qu'implique le dispositif (en direct ou en différé).

La DSTRAT met à disposition un formulaire d'annonce électronique/numérique.

La DSTRAT rend un rapport de son activité au chef EM une fois par année ainsi qu'à chaque fois que les circonstances le commandent.

4.3.4. Statistiques

En application de l'article 16 alinéa 10 RIPAD, la DSTRAT tient des statistiques sur le nombre d'atteintes perpétrées contre des personnes ou des biens que les systèmes de vidéosurveillance de la police ont permis d'établir.

4.4. Sanctions

Le collaborateur qui traite des données personnelles à des fins non professionnelles est, à teneur de l'article 64 LIPAD, passible de l'amende, sans préjudice des peines plus fortes prévues par le droit fédéral (notamment l'article 320 CP sur le secret de fonction).

L'amende est prononcée par le chef du Département.

Par ailleurs, le collaborateur fautif peut faire l'objet d'une procédure disciplinaire.

5. DIFFUSION

5.1. Principes généraux

L'accès, le visionnement des images et l'utilisation des données obtenues au moyen de la vidéosurveillance sont exclusivement réservés au cadre professionnel et sont soumis aux règles sur la protection des données personnelles et sur le secret de fonction.

5.2. Attribution des droits d'accès

Le droit d'accéder aux données est accordé par les chefs de service concernés selon un catalogue de rôles métier correspondant à des droits d'accès à certaines fonctionnalités sur les systèmes de vidéosurveillance (cf. annexes 2 et 3).

Les droits d'accès sont individuels et toutes les connexions se font par comptes nominaux.

Pour des raisons de traçabilité et d'imputabilité des actions, et conformément aux exigences de la LIPAD, les accès par compte générique sont, sauf circonstances exceptionnelles, prohibés.

5.3. Administrateurs des droits d'accès

L'attribution et le retrait des droits sont assurés par le CCSIP. Il convient par conséquent d'informer sans délai le CCSIP de tout changement de personnel affectant la liste des bénéficiaires d'accès.

5.4. Droit d'accès des personnes concernées à leurs données personnelles

Toute personne, collaborateurs de la police inclus, dont les données personnelles sont traitées dans le cadre de la vidéosurveillance peut émettre des prétentions aux conditions prévues par la LIPAD.

Les images issues de la vidéosurveillance étant effacées, sauf exception, à l'issue du délai de conservation, la police n'a pas l'obligation de procéder au floutage d'une personne qui ne serait pas concernée par une affaire mais apparaîtrait sur les images.

5.5. Procédure de marquage d'une séquence d'images capturée par une caméra police ou reliée à la police

Il est de la responsabilité de tout collaborateur de la police informé de la capture par une caméra police ou reliée à la police (cf. chapitre 5.6.), d'un évènement pouvant être utile à l'élucidation d'une affaire, de demander le marquage de la séquence vidéo concernée afin de la préserver contre la destruction automatique résultant de l'expiration du délai initial de conservation.

La demande de marquage se fait au moyen du formulaire Doc. "Demande de préservation d'image ou de séquence de vidéosurveillance".

Tout opérateur de vidéosurveillance est tenu, lorsque demande lui a été faite par un collaborateur de la police ou lorsque lui-même le juge nécessaire et pertinent, d'activer le marquage d'images ou de séquences selon la procédure en vigueur.

En fonction du paramétrage du système, la séquence vidéo marquée est stockée en interne ou sur les serveurs dédiés à la vidéosurveillance.

La durée de la séquence stockée et la durée de conservation du stockage interne dépendent des systèmes et de leurs paramétrages.

Le prolongement du délai de conservation est, en l'état, effectué par extraction sur un support séparé.

5.6. Procédures d'extraction des images ou séquences vidéo

Les procédures d'extraction (cf. annexe 4) dépendent de l'urgence et de la nature de l'évènement pour lequel les images sont requises.

Dans tous les cas, aux fins de traçabilité, le formulaire Doc. "Avis de dépôt de moyen de preuve" doit être rempli.

En cas d'urgence et sur autorisation orale d'une des personnes mentionnées à l'annexe 1, la CVP peut recueillir, traiter, puis transmettre, des images aux policiers par tout moyen électronique validé par le CCSIP. Cette procédure d'urgence est décrite à l'annexe 4.

Le formulaire susmentionné est rempli dans les meilleurs délais.

Pour la transmission d'images, la CVP utilise les moyens informatiques officiels de la police tels que par exemple:

- *Mobile Responder*;
- *Outlook*;
- *Threema*.

5.6.1. Systèmes de caméras hors police

En dehors des caméras que la police gère elle-même, celle-ci est également en mesure d'extraire les images des systèmes suivants :

- caméras de Genève-Aéroport et de son tarmac;
- caméras de la CSI (autoroute et tunnels routiers);
- caméras de l'OFDF;
- caméras de la TPO;
- caméras de l'OCT;
- caméras du stade de la Praille;
- "Cyclope" (évènements majeurs et milieu diplomatique).

L'extraction d'images ou de séquences vidéo se fait au moyen du formulaire 

"Demande d'extraction d'image ou de séquence de vidéosurveillance". Elle doit être soumise à l'autorisation préalable d'une autorité compétente selon le tableau annexé à la présente directive (cf. annexe 1).

Aucun ordre de dépôt n'est demandé.

Les demandes d'extraction émises par la direction de la procédure (MP, TMin ou SDC) sont exécutées d'office par les services compétents. Aucune validation supplémentaire n'est requise.

La procédure d'urgence décrite au point 5.6 s'applique également aux images recueillies dans le présent chapitre.

5.6.2. Autres systèmes

Il s'agit des systèmes pour lesquels la police n'a pas la possibilité d'extraire elle-même les images de vidéosurveillance, soit par exemple :

- les caméras des entreprises privées;
- les caméras des institutions publiques non reliées à la police (Fondation des parkings, TPG, installations communales, etc…);
- les caméras exploitées par des particuliers.

Hors cas de remise volontaire, un ordre de dépôt sera demandé à la direction de la procédure (MP, TMin ou SDC).

En cas d'urgence et de remise volontaire, les policiers peuvent transmettre à la CVP les images recueillies dans ces autres systèmes pour traitement et diffusion. La procédure d'urgence décrite au point 5.6 et dans l'annexe 4 s'applique par analogie.

5.6.3. Frais à la charge de la police

Si, pour fournir à la police des images de vidéosurveillance extraites à sa demande, un particulier ou une société privée encourt à des frais objectifs, il peut en demander la prise en charge ou le remboursement par la police. Cas échéant, ces frais sont portés à la procédure.

Aucune demande de remboursement ne peut être adressée si les images sont extraites à l'initiative du particulier ou de l'entreprise privée.

La demande de remboursement est transmise par le policier en charge à la DFP, accompagnée de l'extraction **myABI** et d'une note explicative validée par sa hiérarchie, en indiquant le numéro de procédure éventuel.

5.7. Communication des données obtenues au moyen de la vidéosurveillance

La communication à des tiers de données obtenues au moyen d'un système de vidéosurveillance ne peut avoir lieu, après validation du COMS, que s'il s'agit de renseigner (article 42 alinéa 4 LIPAD) :

- les autorités judiciaires, soit aux conditions de l'article 39 alinéa 3 LIPAD, soit aux fins de dénoncer une infraction pénale dont la vidéosurveillance aurait révélé la commission;
- les instances hiérarchiques supérieures dont l'institution dépend.