Projet de règlement Curabilis – Vidéosurveillance

Avis du 4 mars 2014

Mots clés: projet de règlement, établissement de détention, vidéosurveillance, protection des données

Contexte: Par courrier électronique du 17 février 2014, Mme Hana Sultan Warnier, Secrétaire générale adjointe du Département de la sécurité et de l'économie (DES), a soumis pour avis au Préposé cantonal à la protection des données et à la transparence (ci-après PPDT) un projet de règlement relatif à l'établissement de détention pour détenus nécessitant des soins psychiatriques Curabilis. Ce projet a été soumis à l'attention du PPDT, en raison de son impact en matière de protection des données personnelles, s'agissant notamment de l'art. 64 sur le système de vidéosurveillance.

Bases juridiques: art. 56 al. 3 let. e LIPAD

Considérations

Le projet de règlement Curabilis

Curabilis est un établissement de mesure fermé au sens de l'art. 377 al. 3 CP, lequel garantit une prise en charge thérapeutique élevée. Le site est composé de 92 places s'articulant autour de quatre unités de mesure, d'une unité hospitalière de psychiatrie pénitentiaire et d'une unité de sociothérapie. Sa mission générale consiste à détenir des personnes majeures, hommes et femmes, privées de liberté en application du droit pénal, du droit administratif ou civil, afin qu'ils reçoivent des traitements, des soins psychiatriques ou de sociothérapie (art. 1 du projet de règlement).

L'instauration de ce lieu de détention doit aller de pair avec **un cadre législatif et réglementaire précis** qui permette une saine application du droit. Des dispositions sont ainsi prévues s'agissant des compétences des multiples intervenants, des différentes unités le composant l'établissement, du régime de détention et de ses sous-aspects, notamment celui relatif aux sanctions et aux pétitions ou plaintes, ainsi que des aspects concernant le Concordat sur l'exécution des peines privatives de liberté et des mesures concernant les adultes et les jeunes adultes dans les cantons latins.

Le libellé de **l'art. 64** (système de vidéosurveillance) est le suivant:

> *[1] Un système de vidéosurveillance est mis en place aux abords et à l'intérieur de Curabilis, dans le respect de l'article 42 de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001.*
>
> *[2] Le directeur de Curabilis édicte une directive précisant les modalités d'utilisation du système de la vidéosurveillance et tient une liste des collaborateurs autorisés à visionner les enregistrements.*

La vidéosurveillance à la lumière du droit public

Parmi tous les dispositifs existant pour surveiller les individus, **la vidéosurveillance** désigne les systèmes techniques permettant d'assurer la surveillance à distance des bâtiments, des biens et des personnes au moyen de caméras vidéo. Ces dernières transmettent les images enregistrées à un poste où elles sont traitées, enregistrées et, éventuellement, visualisées, sur divers supports possibles.

La vidéosurveillance touche immanquablement certains **droits fondamentaux**, particulièrement le droit au respect de la sphère privée et la liberté personnelle (art. 10 al. 2 et 13 Cst., 8 CEDH et 19 Pacte II; voir Cour eur. D.H., *Perry*, du 17 juillet 2003), lesquels protègent notamment l'intégrité physique et psychique d'un individu, sa liberté de mouvement, toutes les informations le concernant qui ne sont pas accessibles au public, les données d'identification et la correspondance privée.

Le recours à **la vidéosurveillance doit respecter ces libertés** de manière générale, que ce soit en droit public ou en droit privé (Flückiger Alexandre/Auer Andreas, La vidéosurveillance dans l'œil de la Constitution, PJA 2006, p. 926).

Les conditions de restrictions de ces libertés sont énumérées à l'art. 36 Cst. Sont exigés: une base légale, un intérêt public et le respect de la proportionnalité et de l'essence des droits fondamentaux.

Suite à l'arrêt rendu par le Tribunal fédéral en la cause 1C.315/2009, du 13 octobre 2010, il convient de préciser que, si une base légale matérielle suffit pour l'installation d'un dispositif de vidéosurveillance qui ne permette pas l'enregistrement des images, une **base légale formelle** est nécessaire pour l'installation d'un dispositif qui le permette.

A Genève, cette base légale formelle est l'art. 42 de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (LIPAD; A 2 08). Cette disposition énonce que la création et l'exploitation d'un système de vidéosurveillance ne sont licites que si, cumulativement, les conditions suivantes sont remplies:

- La vidéosurveillance est 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;
- L'existence d'un système de vidéosurveillance est signalée de manière adéquate au public et au personnel des institutions;
- Le champ de la surveillance est limité au périmètre nécessaire à l'accomplissement de celle-ci;
- Dans l'accomplissement de leurs activités à leur poste de travail, les membres du personnel des institutions publiques n'entrent pas dans le champ de vision des caméras ou, à défaut, sont rendus d'emblée non identifiables par un procédé technique approprié.

L'art. 16 du règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 21 décembre 2011 (RIPAD; A 2 08.01) complète l'art. 42 LIPAD. Il traite précisément de la planification (al. 1), la commission consultative de sécurité municipale (al. 2), l'interconnexion entre systèmes de surveillance (al. 3 et 4), l'inventaire (al. 5 et 6), les établissements scolaires (al. 7), la surveillance du trafic routier (al. 8), la délégation à un tiers (al. 9) et les statistiques (al. 10 à 12).

Quant au respect du principe de **la proportionnalité**, les images enregistrées par les caméras ne peuvent être conservées que pendant un temps limité. Une durée de cent jours, même si elle représente une atteinte non négligeable aux droits fondamentaux des personnes concernées, sera admissible, du moment que les enregistrements issus de la surveillance litigieuse sont exclusivement utilisés dans le cadre d'une procédure pénale (ATF 133 I 88; voir également Cour eur. D.H., *Amann*, du 16 février 2000). La loi genevoise est plus restrictive, car elle dispose que l'éventuel enregistrement de données résultant de la surveillance doit être détruit en principe dans un délai de sept jours, lequel peut être porté à trois mois en cas d'atteinte avérée aux personnes ou aux biens et, en cas d'ouverture d'une information pénale, jusqu'à l'issue de la procédure (art. 42 al. 2 LIPAD).

La vidéosurveillance à la lumière du droit privé

S'agissant de l'utilisation de caméras vidéo à des fins de protection des personnes ou de prévention d'actes de vandalisme par des entreprises privées ou dans le secteur public fédéral, **la loi fédérale sur la protection des données**, du 19 juin 1992 (LPD; RS 235.1) est applicable.

L'exploitation d'un système de vidéosurveillance implique le traitement permanent de données personnelles. Cette forme de surveillance peut en outre, en fonction de la situation, porter sensiblement atteinte à la sphère privée des personnes filmées. Il importe par conséquent d'accorder une attention particulière aux règles de la protection de la personnalité lors de la planification, de l'installation et de l'exploitation de tels systèmes

La loi donne des exemples d'atteintes, parmi lesquels l**a communication à des tiers de données sensibles** (art. 12 al. 2 let. c LPD). On considère notamment comme telles les informations recueillies dans le cadre d'une vidéosurveillance (Flückiger/Auer, op. cit., p. 927).

Le principe est le suivant: **toute atteinte à la personnalité est illicite, à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi** (art. 13 al. 1er LPD; voir Geiser Thomas, Schützt das Arbeitsrecht Journalisten und Journalistinnen genügend?, medialex 2005, p. 201 ss).

Au vu de ce qui précède, la surveillance des abords d'un **établissement pénitentiaire**, comme d'ailleurs de son intérieur, constitue, au vu des impératifs de sécurité, un tel intérêt prépondérant.

Relevons encore que les progrès techniques dans le domaine de la vidéosurveillance permettent non seulement des applications toujours plus complexes, mais également une meilleure **protection de la personnalité** (par exemple codage/chiffrage des images, protection physique contre l'accès non autorisé: 16e Rapport d'activités du Préposé fédéral à la protection des données et à la transparence, 2008/2009, ch. 1.2.1 et 1.2.2; voir aussi l'arrêt du Tribunal administratif fédéral A-7040/2009, du 30 mars 2011 – tous les visages ou plaques de voiture figurant sur les images de *Google Street View* doivent être méconnaissables –).

Les recommandations du Préposé fédéral dans le secteur privé

Selon le Préposé fédéral à la protection des données et à la transparence (http://www.edoeb.admin.ch/datenschutz/00628/00653/00654/index.html?lang=fr), les systèmes de vidéosurveillance ne sont autorisés qu'à condition qu'ils respectent **les principes de licéité et de proportionnalité**. Chaque système de vidéosurveillance doit concrètement remplir les conditions suivantes**:**

- La vidéosurveillance ne peut être effectuée que si les personnes filmées ou susceptibles de l'être y consentent ou si l'atteinte à la personnalité qu'elle représente est justifiée par un intérêt prépondérant public ou privé ou par la loi (principe de la licéité).

Dans la pratique, il est généralement impossible de demander leur accord à toutes les personnes filmées pour exploiter un système de vidéosurveillance. Dans le doute, la vidéosurveillance ne doit être effectuée que s'il existe un intérêt privé ou public prépondérant. Tel est le cas d'un dispositif mis en place à des fins de sécurité.

- La vidéosurveillance doit être un moyen adéquat de réaliser le but poursuivi, à savoir la sécurité (notamment la protection contre les atteintes aux personnes ou aux biens). Elle ne peut être pratiquée que si d'autres mesures moins attentatoires à la vie privée, telles que des verrouillages complémentaires, le renforcement des portes d'entrée ou des systèmes d'alarme, s'avèrent insuffisantes ou impraticables. En outre, les atteintes à la sphère privée causées par la vidéosurveillance doivent se trouver dans un rapport proportionné par rapport au but visé (principe de la proportionnalité). Les caméras factices ne traitent certes pas de données personnelles, mais leur présence donne à penser que tel est le cas. Comme les caméras factices peuvent également s'avérer problématiques pour d'autres raisons juridiques (par ex. pour des questions de responsabilité civile), il est déconseillé de les utiliser.

Quant au **système de vidéosurveillance**, il doit être installé de manière à ce que les principes de la proportionnalité, de la bonne foi et de la transparence soient respectés:

- La caméra doit être installée de manière à ce que n'entrent dans son champ que les images strictement conformes au but de la surveillance (principe de la proportionnalité).
- Le responsable du système de vidéosurveillance doit informer les personnes entrant dans le champ des caméras de l'utilisation d'un tel système au moyen d'un avis bien visible. Au cas où les images sont enregistrées sous quelque forme que ce soit, l'avis doit également indiquer auprès de qui les personnes filmées peuvent faire valoir leur droit d'accès si cela ne ressort pas du contexte (principe de la bonne foi et droit d'accès).

Les principes à respecter lors de l'exploitation d'un système de vidéosurveillance sont au nombre de cinq:

- Les données ne peuvent être utilisées que dans le cadre de la protection contre les atteintes aux personnes ou aux biens. Elles ne peuvent donner lieu à d'autres utilisations (principe de la finalité).
- Le responsable du système de vidéosurveillance doit prendre les mesures organisationnelles et techniques appropriées pour protéger les données personnelles contre tout traitement non autorisé (sécurité des données). Lorsque les images sont transmises par radiocommunication de la caméra au lieu d'enregistrement, le signal doit être crypté ou protégé par d'autres mesures adéquates à même de garantir que des personnes non autorisées ne puissent pas intercepter le signal et visionner les images.
- Le nombre des personnes qui ont accès aux images - que celles-ci soient diffusées en direct ou enregistrées - doit être aussi restreint que possible (sécurité des données et proportionnalité). Il faut en outre déterminer si le but poursuivi par la vidéosurveillance requiert une surveillance en direct ou s'il suffit que les données vidéo enregistrées soient évaluées suite à un événement. Si la seconde option prévaut, les images ne peuvent être visionnées qu'après qu'un événement se soit produit.
- Les données personnelles enregistrées ne doivent pas être divulguées, sauf si les images sont remises à des fins de dénonciation aux autorités de poursuite pénale ou dans des cas prévus ou autorisés par la loi, par exemple lorsqu'un juge en fait la demande (principe de la finalité).
- Les données personnelles enregistrées par une caméra doivent être effacées dans un délai particulièrement bref. Plus les images sont conservées longtemps, plus les exigences en matière de sécurité des données sont élevées. Toute prolongation de la durée de conservation doit être compensée par l'utilisation de technologies permet-

La vidéosurveillance et le domaine pénitentiaire

Interpellée sur la question, **la Préposée vaudoise** à la protection des données et à la transparence a indiqué ne pas voir eu l'occasion de se prononcer sur la vidéosurveillance dans les prisons.

A **Neuchâtel**, la loi sur l'exécution des peines privatives de liberté et des mesures pour les personnes adultes, du 27 janvier 2010 (LPMPA; 351.0) règle la surveillance électronique en ces termes:

> *Art. 86 (cellules)*
> *[1] Les cellules ordinaires des personnes détenues ne font pas l'objet d'une surveillance électronique.*
> *[2] Les cellules disciplinaires et les cellules de sûreté peuvent être surveillées au moyen d'installations électroniques.*
> *[3] Les personnes détenues doivent être avisées de la surveillance en cours.*
>
> *Art. 87 (locaux communs)*
> *Les locaux communs ainsi que le périmètre extérieur des établissements peuvent être surveillés au moyen d'installations électroniques.*
>
> *Art. 88 (enregistrement)*
> *[1] Les informations enregistrées sont effacées après une durée maximale de 7 jours.*
> *[2] Elles sont conservées en cas d'événements particuliers.*
> *[3] Elles peuvent être mises à la disposition des autorités judiciaires.*
> *[4] Au surplus, le Conseil d'Etat règle les modalités.*

A Genève, **en matière pénitentiaire**, les différents règlements sont muets sur la question de la vidéosurveillance (règlement sur le régime intérieur de la prison et le statut des personnes incarcérées, du 30 septembre 1985, RRIP, F 1 50.04; règlement sur l'organisation et le personnel de la prison, du 30 septembre 1985, ROPP, F 1 50.01, règlement du quartier carcéral psychiatrique, du 4 mai 1988, RQCP, F 1 50.16; règlement du centre de sociothérapie «La Pâquerette», du 27 juillet 1988, RPâquerette, F 1 50.20; règlement du centre éducatif de détention et d'observation de la Clairière, du 3 novembre 2004, RClairière, F 1 50.24).

Le Préposé cantonal se demande incidemment si la question de la vidéosurveillance en matière pénitentiaire ne pourrait pas être traitée utilement dans le cadre de la Conférence latine des chefs des départements de justice et police, qui s'intéresse entre autres à la mise en œuvre du Concordat. Certaines recommandations dans le domaine pourraient être formulées à cet égard.

Appréciation de l'art. 64 du projet de règlement Curabilis

L'art. 64 al. 1 du projet de règlement de Curabilis renvoie judicieusement à l'art. 42 LIPAD, lequel constitue à cet égard l'assise légale nécessaire.

L'al. 2, quant à lui, prévoit, à la **première phrase**, qu'il appartient au directeur de préciser les modalités d'utilisation du système de vidéosurveillance. Il conviendra notamment à cet égard de procéder à un recensement de l'ensemble des caméras installées, de limiter le champ des caméras au périmètre nécessaire à la surveillance, ou encore de signaler les caméras

de manière adéquate au public et au personnel. En outre, la directive élaborée devra être accessible au public, en vertu du principe de transparence de l'information.

La seconde phrase de l'al. 2 indique que le directeur tient une liste des collaborateurs autorisés à visionner les enregistrements. Cette précision est importante, puisqu'il est primordial de connaître le nom des personnes compétentes en la matière. A cet égard, le visionnement des images doit être limité à un cercle restreint de personnes dûment autorisées. Il s'agit d'appliquer le système de contrôle dit des quatre yeux, préconisé par le préposé fédéral: un binôme de personnes dûment autorisées est seul habilité à visionner les images lorsque l'atteinte est avérée, et uniquement ensemble. Un ou plusieurs binômes de suppléants, en fonction des circonstances, peuvent être prévus. L'accès au système se fait par une double clé. La loi ne prévoit pas de fonction particulière qui soit requise pour faire partie des personnes autorisées. La liste, qui devra régulièrement être mise à jour, n'a pas à être rendue publique; elle devrait idéalement figurer sur l'Intranet de Curabilis.

Par ailleurs, il est conseillé d'utiliser des **technologies permettant de protéger les données**, par exemple des filtres qui brouillent les visages filmés en temps réel (techniques de floutage) et garantissant donc le respect de la sphère privée. Si les prises servent à des fins d'identification (p. ex. dans le cadre de poursuites pénales), les images filmées peuvent alors être décryptées par les personnes autorisées.

Enfin, il va de soi que le nombre et la disposition des caméras ne doivent **pas servir à surveiller les faits et gestes des employés de Curabilis**.

Avis du Préposé cantonal

Compte tenu de ce qui précède, le Préposé cantonal est d'avis que la formulation de l'art. 64 du projet de règlement Curabilis respecte les principes en vigueur de protection des données.

La directive à venir et la liste des accès constituant une part essentielle du dispositif, il souhaite être tenu informé de la suite des travaux et remarque, à cet égard, que la transparence des mesures prises, la mise à jour régulière des accès accordés, ainsi que la politique d'information et de formation du personnel constitueront des facteurs déterminants de l'acceptabilité de la vidéosurveillance au sein de Curabilis.

Stéphane Werly
Préposé cantonal

Pascale Byrne-Sutton
Préposée adjointe