Les mesures techniques de surveillance

Des risques évités et des risques créés

par

SYLVAIN MÉTILLE*

1. Introduction

1.1 Les risques

Qu'est-ce qu'un risque? On ne trouve pas dans la jurisprudence du Tribunal fédéral une définition unique du risque, tant les risques sont nombreux et variés,

* Avocat et doctorant à Neuchâtel.

mais aussi parce que les situations dans lesquels ils sont appréhendés sont nombreuses et variées[1].

Le Petit Robert définit le risque comme l'éventualité d'un événement ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage. Cette définition est suffisante pour la présente contribution. Nous examinerons essentiellement les risques que les mesures de surveillance tentent de combattre et les risques créés par les mesures de surveillance.

1.2 Les cas de surveillance

Par mesure de surveillance technique, on entend toute méthode utilisée par l'homme au moyen d'un appareil lui permettant d'écouter, d'observer, de localiser, d'identifier ou de recueillir de n'importe quelle manière des informations sur un individu ou un lieu[2]. Trois cas de surveillance seront abordés: la surveillance pénale, la surveillance préventive et finalement la surveillance dissuasive.

La surveillance pénale intervient au stade de l'enquête, plus précisément au stade de la procédure préliminaire[3]. Ces mesures de surveillance sont actuellement régies par la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et les codes cantonaux de procédure pénale. Dès l'entrée en vigueur au 1er janvier 2011 du Code de procédure pénale au niveau fédéral (CPP), les cantons n'auront plus de compétences législatives en la matière.

---

1 Les risques suivants ressortent de la jurisprudence fédérale: réalisation du risque assuré, risque d'abus, risque de confusion, étude de risque, risque de passage à la clandestinité, risque pour un tiers, risque normal d'exploitation, principe du risque admissible, théorie du risque accru, risque de préjudice pour la forêt, profits et risques, risque de collusion, analyse des risques, risque de passage à l'acte, risque d'insolvabilité, répartition des risques prévue, mesure de la diligence en cas d'accumulation des risques, garantie contre les risques à l'exportation, risque inhérent à l'emploi du véhicule, risque que représente l'assuré, répartition légale des risques entre tireur et tiré, conséquences de l'absence d'annonce en cas d'augmentation du risque, risque inhérent à l'emploi, réalisation du risque assuré, risque de récidive, sélection des risques, compensation des risques, risque de fuite, etc.

2 Pour une définition légèrement plus restrictive: GISLER F., *La coopération policière internationale de la Suisse en matière de lutte contre la criminalité organisée*, in: P. Gauch (éd.), *Travaux de la Faculté de droit de l'Université de Fribourg*, Zurich, 2009, p. 90; RHYNER B./ STÜSSI, D., *«Kommentar zu Art. 269-279 StPO»*, in: G. Albertini/B. Fehr,/B. Voser (éds), *VSKC-Handbuch*, Zurich, 2008, pp. 435-436. Pour des exemples de mesures de surveillance visibles: CUSSON M., *«La surveillance et la contre-surveillance»*, in: M. Cusson/B. Dupont/ F. Lemieux (éds), *Traité de sécurité intérieure*, Lausanne, 2008, pp. 429-432.

3 Au sens où l'entend le CPP. L'investigation préalable connue par certains cantons n'existera plus avec la procédure unifiée: CONSEIL FÉDÉRAL, Message relatif à l'unification du droit de la procédure pénale du 21 décembre 2005, publié in FF 2005 1057, pp. 1247-1248.

La surveillance préventive est généralement opérée en dehors de toute procédure judiciaire[4]. C'est notamment celle qui est effectuée par les services de renseignements civils et militaires[5]. Le Service d'analyse et de prévention (SAP)[6] est notamment chargé de détecter précocement les dangers liés au terrorisme, au service de renseignements prohibé, à l'extrémisme violent, au commerce illicite d'armes et de substances radioactives ainsi qu'au transfert illégal de technologie. Ces activités de surveillance sont réglées par la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[7]. La surveillance préventive est mise en place lorsqu'il existe un soupçon de menace significative pour la sécurité, alors que la poursuite pénale est engagée lorsqu'il y a une infraction concrète. La sécurité intérieure de la Suisse pouvant être menacée tant par des actes non punissables pénalement que par des actes répréhensibles, les investigations préventives peuvent découler indifféremment de ces deux catégories d'actes[8].

Si en matière de surveillance pénale et de surveillance préventive, on a le plus souvent à faire à des mesures de surveillance invasives, soit des mesures secrètes[9], la surveillance mise en place par des personnes à titre privée l'est souvent dans un

---

4 On distingue le renseignement pénal (judiciaire) du renseignement de sécurité (politique): LEMAN-LANGLOIS S./LEMIEUX, F., *«Renseignement de sécurité et renseignement criminel»*, in: M. Cusson/B. Dupont/F. Lemieux (éds), *supra* note 2, p. 336.

5 Sur la délimitation des tâches entre le service de renseignement intérieur et les autorités de poursuite pénale: CONSEIL FÉDÉRAL, Rapport donnant suite au postulat du 21 février 2005 de la Commission de la politique de sécurité du Conseil des Etats (05.3006) du 9 juin 2006, publié in FF 2005 5421, pp 5437-5438. Sur l'organisation des services de renseignement suisses et leurs attributions respectives: OFFICE FÉDÉRAL DE LA POLICE (FEDPOL), *Rapport explicatif à l'avant-projet de révision de la Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)*, Berne, 2006, pp. 6-12; WEISSEN R., *Les services de renseignement suisses*, Secrétariat général du DDPS, Berne, 2004, pp. 24-47. Sur la notion de renseignement et les différents buts poursuivis par le renseignement: BRODEUR J.-P., *«Le renseignement I: concepts et distinctions préliminaires»*, in: M. Cusson/B. Dupont/F. Lemieux (éds), *supra* note 2, pp. 263-277; CUSSON M., *supra* note 2, p. 48; LEMIEUX F., *«Vers un renseignement criminel de qualité»*, in: M. Cusson/B. Dupont/F. Lemieux (éds), *supra* note 2, pp. 292-295.

6 Rattaché au Département fédéral de la défense, de la protection de la population et des sports (DDPS).

7 Le Code de procédure pénale ne s'applique qu'aux activités de la police en matière de poursuite pénale. Les activités qui relèvent de la sûreté n'y sont pas soumises: CONSEIL FÉDÉRAL, Message relatif à l'unification du droit de la procédure pénale du 21 décembre 2005, publié in FF 2005 1057, p. 1112.

8 CONSEIL FÉDÉRAL, Message relatif à la modification de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure du 15 juin 2007, publié in FF 2007 4773, pp. 4797-4798.

9 Sur la distinction entre la vidéosurveillance d'observation, la vidéosurveillance dissuasive et la vidéosurveillance invasive: BAERISWYL B., *«Videoüberwachung – im rechtsfreien Raum?, Datenschutzrechtliche Aspekte moderner Überwachung mittels optischen Geräten»*, digma 2002 (1), pp. 26-27; DFJP, *Vidéosurveillance exercée en vue d'assurer la sécurité dans les gares, les aéroports et les autres espaces publics* 2007, p. 9; FLÜCKIGER A./AUER, A., *«La vidéosurveillance dans l'œil de la constitution»*, AJP/PJA 2006 (8), pp. 924-925.

but d'observation[10] ou dans un but dissuasif[11]. Les dispositifs de vidéosurveillance placés dans des lieux accessibles au public et dont le but est de rassurer tout autant que d'éviter la commission d'infractions en sont un bon exemple.

2. Les risques visés selon le cas de surveillance

2.1 L'infraction pénale commise

La surveillance pénale porte sur une infraction déjà réalisée, éventuellement une infraction continue en cours de réalisation[12]. Il ne s'agit plus d'un risque à proprement parler vu que l'éventualité redoutée s'est déjà produite[13].

Les mesures de surveillance prévues par le CPP ont pour but de rechercher l'auteur de l'infraction ou de prouver l'existence de l'infraction. Elles ne sont admises que si une infraction a été commise et s'il existe des soupçons suffisants[14]. Cela rend les mesures de surveillance admissibles, puisqu'elles sont basées sur des faits objectifs et vérifiables que la surveillance n'influence pas. Par conséquent, la recherche indéterminée de preuves est exlue[15].

Une mesure de surveillance ne doit pas servir à créer un soupçon[16]. Le CPP ne prévoit pas la surveillance à titre préventif. La commission d'actes préparatoires

---

10 On parle de surveillance d'observation lorsqu'elle est utilisée pour surveiller un rayon déterminé accessible au public, afin de constater des mouvements ou des phénomènes objectifs. Ce genre de surveillance revêt plutôt un caractère organisationnel ou de gestion de l'espace, par exemple pour contrôler la fluidité du trafic routier.

11 La surveillance dissuasive consiste à surveiller ouvertement un lieu pour tenter de dissuader les personnes qui s'y trouvent de commettre des infractions. C'est souvent sa visibilité qui la rend efficace.

12 Notamment en matière de trafic de stupéfiants, où ce n'est pas tant les délits commis qui sont visés, mais ceux qui sont en cours et le réseau existant. Pour un avis critique: RUCKSTUHL N., *«Technische Überwachungen aus anwaltlicher Sicht»*, Pratique juridique actuelle 2005 (2), p. 150.

13 Sous réserve du risque de récidive, mais qui ne serait pas propre à justifier une mesure de surveillance.

14 De manière générale l'art. 197 al. 1 lit. b CPP et pour des exemples les art. 255, 256, 269, 273, 282 et 284 CPP.

15 Aussi appelée «fishing expedition», soit des actes d'enquêtes motivés par aucun soupçon, mais dont le but est des découvrir au hasard des infractions ou des indices propres à fonder un soupçon.

16 GOLDSCHMID P., *Der Einsatz technischer Überwachungsgeräte im Strafprozess: unter besonderer Berücksichtigung der Regelung im Strafverfahren des Kantons Bern*, Berne, 2001, p. 95; HANSJAKOB T., *BÜPF/VÜPF: Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*, St. Gallen, 2006, p. 145.

n'ouvre la voie à des mesures de surveillance que s'il s'agit d'une infraction propre, soit des actes préparatoires délictueux au sens de l'art. 60bis CP[17].

2.2 La menace pour la sécurité intérieure

Les mesures de surveillance fondées sur la LMSI, notamment la recherche d'informations relatives à la sûreté intérieure et extérieure, doivent permettre de prendre des mesures préventives pour mettre à jour et cas échéant écarter les menaces. Le but est donc d'éviter la réalisation d'un risque pour la sécurité intérieure. La justification de la surveillance n'est pas tant un élément existant, mais plutôt une projection, un risque futur. Elle trouve pourtant sa justification dans des faits déjà réalisés.

Les informations recherchées doivent être nécessaires à prévenir et lutter contre les dangers liés au terrorisme, au service de renseignements prohibé, à l'extrémisme violent ou à la violence lors de manifestations sportives[18]. La surveillance doit ensuite reposer sur des soupçons[19]. Un soupçon qualifié (la loi parle d'une présomption sérieuse) est exigé lorsque la surveillance porte sur des informations relatives à l'engagement politique ou à l'exercice des droits découlant de la liberté d'opinion, d'association et de réunion[20]. L'exploitation de ces informations est également plus restreinte[21].

Les moyens de surveillance légalement utilisables sur la base de la LMSI sont actuellement limités. Le recours à des mesures de contrainte et l'observation de faits dans des locaux privés sont interdits, de même que la surveillance de la cor-

---

17 Constituent des infractions punissables en tant que telles les actes préparatoires en vue des infractions suivantes: meurtre (art. 111 CP), assassinat (art. 112 CP), lésions corporelles graves (art. 122 CP), brigandage (art. 140 CP), séquestration et enlèvement (art. 183 CP), prise d'otage (art. 185 CP), incendie intentionnel (art. 221 CP), et génocide (art. 264 CP). En matière d'infractions à la LStup, l'art. 19 ch. 1 al. 6 LStup prévoit que les mesures prises en vue du trafic de stupéfiants sont des délits indépendants. Ils incluent aussi bien la tentative que certains actes préparatoires (ATF 121 IV 198, 200, S., du 19 septembre 1995).

18 Art. 2 et 14 LMSI.

19 OFFICE FÉDÉRAL DE LA POLICE (FEDPOL), *Rapport explicatif à l'avant-projet de révision de la Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)*, Berne, 2006, p.6,.

20 Présomption sérieuse permettant de soupçonner une organisation ou des personnes qui en font partie de se servir de l'exercice des droits politiques ou des droits fondamentaux pour dissimuler la préparation ou l'exécution d'actes relevant du terrorisme, du service de renseignements ou de l'extrémisme violent (art. 3 al. 1 LMSI).

21 Si les soupçons relatifs à un comportement punissable ne sont pas corroborés par les activités observées, les informations recueillies ne peuvent pas être enregistrées avec référence nominale. Les prises de vues et les enregistrements sonores doivent alors être détruits dans un délai de 30 jours (art. 3 al. 1 LMSI).

respondance et des télécommunications[22]. L'État ne bénéficie actuellement pas du droit de procéder à une surveillance préventive de manière beaucoup plus étendue qu'une personne privée[23]. Il bénéficie en revanche de compétences nettement plus larges en matière de traitement des informations dont il dispose.

La limitation juridique des possibilités d'atteinte à la sphère privée de l'individu est motivée essentiellement par le fait que la personne surveillée n'a pas commis d'infraction. Elle ne dispose pas non plus des moyens de remettre en cause la surveillance dont elle ferait l'objet, ces mesures n'étant pas soumises à un contrôle judiciaire similaire à celui de la procédure pénale.

Des moyens plus étendus sont prévus dans un projet de révision de la LMSI (LMSI II)[24]. L'avenir de cette révision est très incertain. Alors que le Conseil national a refusé l'entrée en matière[25], le Conseil des États est entrée en matière mais a renvoyé le projet au Conseil fédéral[26].

Le projet prévoit notamment la surveillance de la correspondance par poste et télécommunication, la surveillance (à l'aide d'appareils techniques) de lieux qui ne sont pas librement accessibles, mais il ne prévoit pas la surveillance des relations bancaires. Ces moyens seraient soumis à un double contrôle: à la demande de l'Office fédéral de la police, le Tribunal administratif fédéral examinera si les mesures sont conformes au droit, puis le chef du Département fédéral de justice et police (DFJP) et le chef du Département fédéral de la défense, de la protection de la population et des sports (DDPS) examineront ensuite la demande sous l'angle politique et décideront d'un commun accord des mesures à mettre en place[27].

La nouveauté de ce projet n'est pas tant les moyens de surveillance qui sont déjà connus de la procédure pénale, mais la possibilité de les utiliser avant la commission d'une infraction, voire en l'absence totale de projets de commettre une infrac-

---

22 CONSEIL FÉDÉRAL, Analyse de la situation et des menaces pour la Suisse à la suite des attentats terroristes du 11 septembre 2001, rapport du Conseil fédéral à l'intention du Parlement du 26 juin 2002, publié in FF 2003 1674, pp. 1715-1716.

23 MÉTILLE S., *«L'utilisation privée de moyens techniques de surveillance et la procédure pénale»*, in: J.-P. Dunand/P. Mahon (éds), *«Le droit décloisonné», interférences et interdépendances entre droit privé et droit public, Enseignements de 3e cycle de droit*, Genève/Zurich/Bâle, 2009.

24 Contrairement à ce qui se fait habituellement, ce projet de révision de la LMSI II a débuté par la publication par l'Office fédéral de la police d'un avant-projet (OFFICE FÉDÉRAL DE LA POLICE (FEDPOL), *Rapport explicatif à l'avant-projet de révision de la Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)*, Berne, 2006). Le Conseil fédéral a ensuite publié le projet de modification de la loi accompagné d'un message le 15 juin 2007, suivant en cela la procédure usuelle (CONSEIL FÉDÉRAL, Message relatif à la modification de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure du 15 juin 2007, publié in FF 2007 4773-4872.).

25 Par 92 voix contre 79 le 17 décembre 2008: BO 2008 N 1885-1892.

26 Le 3 mars 2009: BO 2009 E 19-21.

27 CONSEIL FÉDÉRAL, Message relatif à la modification de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure du 15 juin 2007, publié in FF 2007 4773, p. 4804.

tion. Bien qu'une procédure précise avec apparemment de nombreux contrôles soit prévue, il n'en demeure pas moins que le projet LMSI II a pour but de réintroduire les mesures de surveillance préventive que le législateur avait précédemment exlues[28]. Il s'agit de développements inquiétants qui mettent en danger plusieurs droits et libertés fondamentaux[29].

2.3 L'infraction potentielle et l'insécurité

Des motivations variées conduisent à la mise en place de mesures de surveillance privées. Il s'agit le plus souvent d'empêcher la réalisation d'un risque grâce à l'effet dissuasif de la surveillance, comme lors de la mise en place de caméras[30]. Il s'agit parfois de vérifier des soupçons, comme lors de l'engagement d'un détective.

La surveillance dissuasive a pour but d'éviter la réalisation d'un risque, qu'il soit réel ou supposé. Lorsqu'il n'y a pas de risque objectif, la surveillance a surtout pour but et pour effet de rassurer, en luttant contre l'insécurité ressentie[31]. Le risque dont il est ici question revêt des formes très variées, allant d'un comportement non désiré (accès à un local, utilisation d'un appareil, mauvaise exécution du travail, etc.) à la commission d'une infraction pénale, en passant par l'enregistrement de données pour une éventuelle utilisation ultérieure (vérification, preuve, etc.).

---

28 Sur l'histoire de la surveillance préventive en Suisse et l'affaire dite des fiches en particulier: KREIS G., *«Staatsschutz im Laufe der Zeit»*, digma 2009 (2), pp. 54-59; KREIS G./DELLEY J.-D./KAUFMANN O. K., [*et al*.], *La protection politique de l'Etat en Suisse: l'évolution de 1935 à 1990; étude pluridisciplinaire effectuée et éditée sur mandat du Conseil fédéral*, Berne, 1993.

29 CESONI M. L., *«Droit pénal européen et dérives de l'antiterrorisme»*, Plaidoyer 2008, Vol. 5, p. 56.

30 L'important est que l'auteur du risque potentiel se sente surveillé et renonce à son projet. Que la surveillance soit effective ou non ne joue souvent pas de rôle. C'est pour cette raison qu'il existe parfois des leurres, comme de fausses caméras.

31 Sur la distinction entre le risque objectif et le sentiment d'insécurité: KUHN A., *Sommes-nous tous des criminels?*, Grolley, 2002, pp. 29-30. Sur le sentiment d'insécurité en général: VIREDAZ B., *Le sentiment d'insécurité: devons-nous avoir peur?*, Grolley, 2005. Pour une évaluation des effets de la vidéosurveillance: GILL M./SPRIGGS A., *Assessing the impact of CCTV*, Home Office Research, Development and Statistics Directorate n° 292, Londres, 2005; WELSH B. C./FARRINGTON D. P., *Crime prevention effects of closed circuit television: a systematic review*, Home Office Research, Development and Statistics Directorate n° 252, Londres, 2002.

3. Quelques risques créés par la surveillance

3.1 L'atteinte à la sphère privée

Les mesures de surveillance peuvent porter atteinte à la protection de la sphère privée (art. 13 al. 1 Cst, 8 CEDH et 28ss CC), mais également à d'autres droits fondamentaux, parmi lesquels la liberté personnelle (art. 10 Cst), la protection des données (art. 13 al. 2 Cst et la LPD) et évidemment le secret de la correspondance et des télécommunications (art. 13 al. 1 Cst, 8 CEDH et art. 179ss CP).

La liberté personnelle recouvre l'intégrité physique et psychique, ainsi que la liberté de mouvement[32]. La protection de la vie privée permet à toute personne de mener sa vie selon son propre choix, de choisir son mode de vie, d'organiser ses loisirs et d'avoir des contacts avec autrui sans intervention des pouvoirs publics. On parle aussi du droit de vivre autant qu'on le désire à l'abri des regards étrangers[33].

La Cour européenne des droits de l'homme retient que la protection de la vie privée est principalement destinée à assurer le développement, sans ingérence, de la personnalité de chaque individu dans ses relations avec ses semblables[34]. Le droit au respect de la vie privée protège l'ensemble des informations relatives à une personne qui ne sont pas accessibles au public, notamment des données d'identification, des données concernant un traitement médical, l'identité sexuelle, la participation à une association ou encore les dossiers de procédures judiciaires. L'enregistrement d'images de surveillance prises sur des places ou des voies pu-

---

32 AUBERT J.-F./MAHON P., *Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999*, Zurich/Bâle/Genève, 2003, pp. 100-122; AUER A./MALINVERNI G./HOTTELIER, M., *Droit constitutionnel suisse II*, Berne, 2006, pp. 143-182; BAUM O., «Rechtliche Fragestellungen im Zusammenhang mit dem kriminalpräventiven Einsatz von Videoüberwachungsanlagen im öffentlichen Raum»,Jusletter 8 octobre 2007, disponible sur le site: www.weblaw.ch; BIAGGINI G., *BV: Bundesverfassung der Schweizerischen Eidgenossenschaft und Auszüge aus der EMRK, den UNO-Pakten sowie dem BGG*, Zurich, 2007, pp. 121-125; HÄFELIN U./HALLER, W./KELLER H., *Schweizerisches Bundesstaatsrecht*, Zurich, 2008, pp. 105-116; KIENER R./KÄLIN W., *Grundrechte*, Berne, 2007, pp. 125-145; RHINOW R. A./SCHEFER, M., *Schweizerisches Verfassungsrecht*, Bâle, 2009, pp. 253-256.

33 AUBERT/MAHON, *supra* note 32, pp. 123-135; AUER/MALINVERNI/HOTTELIER, *supra* note 32, pp. 184-189; BAUM, *supra* note 32; BIAGGINI, *supra* note 32, pp. 312-134; HÄFELIN/HALLER/KELLER, *supra* note 32, pp. 117-120; KIENER/KÄLIN, *supra* note 32, pp. 148-149; RHINOW R., *Grundzüge des schweizerischen Verfassungsrechts*, Bâle/Genève/Munich, 2003, pp. 221-223.

34 Arrêt Botta c. Italie du 24 février 1998, no 21439/93, § 32, CEDH 1998-I. La Cour rattache à la protection de la sphère privée la protection de l'intégrité physique et l'intégrité morale, ainsi que la protection des données.

bliques et la conservation de ces enregistrements portent atteinte à la sphère privée[35].

La conservation de données personnelles non accessibles au public peut également constituer une atteinte, quand bien même ces données auraient été collectées sans violation du droit constitutionnel et que les informations recueillies correspondraient aux faits[36]. La Cour européenne des droits de l'Homme a précisé que des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics[37].

Pour mémoire, une atteinte à un droit fondamental est admissible si elle respecte les conditions de l'art. 36 Cst. Toute restriction d'un droit fondamental doit être fondée sur une base légale, justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui et proportionnée au but visé. L'essence des droits fondamentaux est en outre inviolable et les restrictions graves doivent être prévues par une loi[38].

Le droit au respect de la correspondance, ainsi que des relations établies par la poste et les télécommunications sont un autre aspect essentiel de la sphère privée. Il couvre l'ensemble des communications qu'une personne peut établir avec autrui, indépendamment du vecteur utilisé[39].

3.2 L'utilisation de données à l'insu de la personne concernée

La protection des données et l'autodétermination informationnelle donnent le droit à toute personne d'être protégée contre l'emploi abusif de données personnelles qui la concernent. Elle implique le droit d'être informée de l'existence de telles

---

35 ATF 133 I 77, 80, Diggelmann, du 14 décembre 2006.

36 ATF 122 I 360, 362, B. et consorts, du 28 nombre 1996.

37 Arrêt Rotaru c. Roumanie du 4 mai 2000 (exceptions préliminaires) [GC], no 28341/95, § 43, CEDH 2000-V.

38 Sur la théorie générale de restrictions des libertés: AUBERT/MAHON, *supra* note 32, pp. 319-331; AUER/MALINVERNI/HOTTELIER, *supra* note 32, pp. 79-119; BIAGGINI, *supra* note 32, pp. 75-109; HÄFELIN/HALLER/KELLER, *supra* note 32, pp. 90-101; RHINOW/SCHEFER, *supra* note 32, pp. 237-245; SCHWEIZER R. J., *«Kommentar zu Art. 36 BV»*, in: B. Ehrenzeller/ P. Mastronardi/R. J. Schweizer [*et al.*] (éds), *Die schweizerische Bundesverfassung Kommentar*, Zurich, 2008, pp. 727-742.

39 Communication orale, écrite, par voie de poste, télégraphe, téléfax, téléphone, réseau électronique, etc. Les documents déjà parvenus à leur destinataire ne sont en revanche plus couverts par le secret de la correspondance. L'identification de l'utilisateur, de l'interlocuteur et du raccordement téléphonique, le moment et la durée de la conversation, ainsi que les adresses et la période à laquelle un utilisateur a envoyé ou reçu des messages sont également protégés: ATF 126 I 50, 62-63, Swiss Online AG, du 5 avril 2000, et ATF 130 III 28, 32, A., du 21 octobre 2003.

données et d'obtenir la rectification des données inexactes et la suppression des données inutiles. Par données personnelles, on entend toute information sur les caractéristiques physiques, psychiques, sociales ou politiques d'un individu, indépendamment du support utilisé. Les droits garantis concernent les données de base, telles qu'elles sont enregistrées, mais également celles qui résultent de leur traitement, soit les analyses et appréciations faites sur la base de ces données et consignées dans des dossiers[40].

Des données peuvent également être utilisées, y compris légalement, sans que la personne concernée ne s'en rende compte. On peut ici penser au futur employeur qui effectue une recherche sur l'Internet au sujet d'un candidat. Il est impossible pour un individu de vérifier toutes les données qui peuvent être recueillies sur son compte, même en se limitant aux données qui peuvent être récoltées légalement. Les données consultées peuvent également avoir été recueillies secrètement, rendant alors totalement impossible un éventuel contrôle de la personne concernée.

L'utilisation du droit d'accès garanti par l'art. 8 de la Loi fédérale sur la protection des données (LPD) oblige à s'adresser indépendamment à chaque maître de fichier individuellement. Il en est de même pour l'exercice du droit de rectification des données inexactes (art. 5 LPD). Il faut donc connaître l'existence du fichier et du maître de celui-ci et adresser de multiples demandes, auxquelles il n'est pas toujours donné la suite adéquate. Même dans les cas de bases de données étatiques, il est difficile pour l'administré de s'y retrouver[41].

3.3 L'impossibilité de corriger des données inconnues

A première vue cela paraît être une évidence: il n'est pas possible de corriger les données que l'on ne connaît pas. Les conséquences sont pourtant grandes et souvent mésestimées. Comme nous l'avons vu précédemment il faut avoir connaissance de l'existence des données et savoir qu'elles ont été ou pourraient être utilisées pour faire valoir les droits découlant de la LPD. Mais on trouve des situations encore plus compliquées, où un droit d'accès en tant que tel n'existe pas[42].

Dans certains cas particuliers où la LPD n'est pas applicable, on ne retrouve qu'un droit d'accès indirect. C'est par exemple le cas pour les données inscrites dans le

---

40 AUBERT/MAHON, *supra* note 32, pp. 130-131; AUER/MALINVERNI/HOTTELIER, *supra* note 32, pp. 187-189; BIAGGINI *supra* note 32, pp. 134-136; BREITENMOSER S., *«Kommentar zu Art. 13 BV»*, in: B. Ehrenzeller/P. Mastronardi/R. J. Schweizer [*et al.*] (éds), *supra* note 38, pp. 306-334; GRAFFENRIED P. D., *Actes de la Police judiciaire*, Thèse, Lausanne, 1981, pp. 141-143; HÄFELIN/HALLER/KELLER, *supra* note 32, pp. 119-120; KIENER/KÄLIN, *supra* note 32, pp. 158-161; RHINOW, *supra* note 33, pp. 227-228.

41 RIKLIN F., *«Vollzugsdefizite noch und noch»*, plädoyer 2009, Vol. 3, p. 22.

42 Sans mentionner ici les problèmes qui peuvent en plus se poser lorsqu'un fichier est situé et géré de l'étranger.

système de traitement des données relatives à la protection de l'Etat (ISIS)[43]. La LMSI ne prévoit pas d'information de la personne surveillée, mais celle-ci jouit d'un droit de contrôle. Toute personne peut saisir le Préposé fédéral à la protection des données et à la transparence (PFPDT) pour qu'il vérifie si des données la concernant sont traitées conformément au droit dans ce système d'information du Service d'analyse et de prévention (SAP).

Bien que l'on parle parfois d'un droit d'accès indirect, il ne s'agit en réalité pas d'un droit de la personne concernée d'être renseignée, mais seulement d'un contrôle administratif particulier et indépendant. Le Préposé a accès à l'ensemble des informations, mais il ne les transmettra pas à la personne concernée. En principe il répondra avec un libellé standard confirmant qu'aucune donnée la concernant n'a été traitée illégalement ou que, dans le cas d'une éventuelle erreur dans le traitement des données, il a adressé au SAP la recommandation d'y remédier. Cette communication ne doit pas permettre au destinataire de déduire si des informations ont été recueillies sur son compte ou pas[44].

Ce droit d'accès indirect oblige pourtant le Service d'analyse et de prévention à vérifier que les informations existantes restent nécessaires et à effacer toutes celles qui le ne sont pas, même si le délai prévu de conservation n'est pas atteint. Par ailleurs, les personnes recensées qui ont saisi le Préposé fédéral à la protection des données et à la transparence seront renseignées dès lors que les intérêts liés au maintien de la sûreté intérieure n'exigent plus le secret ou au plus tard lors de l'expiration de l'obligation de conserver les données (art. 18 al. 5 et 6 LMSI)[45].

Le Préposé n'a accès qu'aux informations que lui transmet l'autorité contrôlée et il ne peut évidemment pas contrôler la véracité des données recueillies, par exemple en s'entretenant avec la personne surveillée[46].

La Conseillère nationale Susanne Leutenegger Oberholzer a déposé une motion le 17 décembre 2008 demandant à ce qu'un droit d'accès aux données conforme aux art. 8 et 9 LPD soit garanti pour tous les fichiers de la Confédération[47]. Ce droit d'accès est connu dans tous les cantons et il est la seule possibilité de permettre une rectification des données erronées. Dans sa réponse du 13 mars 2009, le Conseil fédéral admet que le droit d'accès indirect est problématique et qu'il ne consti-

---

43 ISIS (Staatsschutz-Informations-System), basé sur l'Ordonnance du 30 novembre 2001 sur le système de traitement des données relatives à la protection de l'Etat (RS 120.3).

44 PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *14ème rapport d'activités 2006/2007*, Office fédéral des constructions et de la logistique, Berne, 2007, pp. 39-41; PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *15ème rapport d'activités 2007/2008*, Office fédéral des constructions et de la logistique, Berne, 2008, pp 44-46.

45 Pour les fichiers soumis à la LSIP, les personnes au sujet desquelles aucune donnée n'a été traitée en sont informées par fedpol trois ans après réception de leur demande (art. 8 al. 7 LSIP).

46 BUSCH H., *«Frei Bahn für den Staatsschutz»*, Plaidoyer 2007, Vol. 3, p. 18.

47 Ce qui conduirait à une modification des art. 8 et 11 al. 6 LSIP et 18 LMSI.

tue pas un vrai droit d'accès. Il considère qu'un droit d'accès au sens de l'art. 8 LPD doit être garanti à toute personne dont les données personnelles sont collectées, y compris dans les domaines de la sécurité intérieure et de l'information policière, les exceptions devant être fixées dans le cadre de l'art. 9 LPD[48]. Cette motion a malheureusement été rejetée le 3 mars 2010 par le Conseil national par 95 voix contre 64 (BO 2010 N 141).

En pratique, la protection des données sert de nos jours plutôt à corriger des données fausses, y compris celles que l'on a volontairement rendues accessibles, qu'à interdire la divulgation des données comme c'était le but à l'origine.

3.4 La sécurité des données, les fuites et la transmission des données

Une mesure de surveillance produit la plupart du temps des résultats sous la forme de données, dont l'exploitation consciente peut constituer un risque pour certains droits fondamentaux comme nous l'avons vu précédemment. Ces données peuvent également être utilisées de manière inadéquate à cause d'erreurs humaines ou techniques, voire être utilisées par des personnes qui ne devraient pas y avoir accès.

Le risque existe que des serveurs subissent des pannes ou des attaques informatiques (piratage, codes malicieux, virus, etc.) qui entraînent la perte, la destruction ou le vol de données[49]. Ces données peuvent aussi être endommagées. Au niveau des dysfonctionnements techniques, on relèvera également le cas des fausses alertes, notamment avec les processus automatisés[50]. La vidéosurveillance connaît de nombreuses utilisations entièrement automatiques, comme la détection d'incendies, la signalisation d'objets immobiles ou en mouvement, la détection de contresens sur une autoroute, l'identification de véhicules et de plaques d'immatriculation, la détection d'une mallette abandonnée dans un couloir, la détection d'une tentative de suicide le long des voies de métro, ou encore l'absence de mouvement d'un corps flottant entre deux eaux dans une piscine[51]. Si ces processus étaient

---

48 CONSEIL FÉDÉRAL, Réponse à la motion 08.3852 déposée par la Conseillère nationale Leutenegger Oberholzer du 13.03.2009.

49 BONDALLAZ S., Le «droit à une télécommunication protégée» ou la nécessité de reconsidérer la protection de la vie privée dans les environnements numériques, Jusletter 25 février 2008, disponible sur le site: www.weblaw.ch.

50 Dans le même sens la problématique des faux positifs en matière de reconnaissance biométrique par exemple: COMMISSION D'ACCÈS À L'INFORMATION (CAI), *La biométrie au Québec: les enjeux*, Québec, 2002, p. 20; DIDIER B., *«Biométries»*, in: OCDE (éd.), *L'économie de la sécurité*, Paris, 2004, pp 43-44; PRIVATIM, *Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données*, Zurich, 2006, p. 6.

51 Pour des exemples: FLÜCKIGER/AUER, *supra* note 9, p. 925; RUEGG J./FLÜCKIGER A./NOVEMBER V. [*et al*]., *Vidéosurveillance et risques dans l'espace à usage public: représentations des risques, régulation sociale et liberté de mouvement*, Travaux du CETEL, 2006,

confiés à un opérateur humain, le risque d'erreur existerait également. Si le risque d'erreur est réduit par les plus grandes compétences de l'opérateur, un opérateur devant surveiller seuls plusieurs dizaines d'écrans de surveillance ne peut simplement pas tout voir en même temps. La machine peut alors présélectionner automatiquement les éléments nécessitant éventuellement une intervention humaine, puis l'opérateur effectuer un second contrôle et décider de la juste mesure à prendre.

La communication des données constitue un autre risque important. Une fois celles-ci diffusées, le propriétaire originel n'en a plus aucune maîtrise. On connaît la mémoire d'internet et des supports informatiques[52]. A nouveau la communication de données peut intervenir automatiquement ou à la suite d'une instruction humaine. Les données peuvent aussi être récupérées par une personnes qui n'est pas censée y avoir accès. Des formes toujours plus professionnelles de cybercriminalité existent désormais, au point de constituer un véritable marché organisé et lucratif[53]. Très souvent la simple curiosité est à l'origine d'un accès indu. La tentation est d'autant plus grande que des mesures élémentaires pour limiter l'accès font souvent défaut. Les situations ou n'importe qui peut accéder au résultat d'une vidéosurveillance ou des fichiers de données quelconques sur un ordinateur ou via un réseau informatique sont fréquentes. Les mêmes réflexions s'appliquent à l'intégrité des données, qui pourraient être modifiées par celui qui arrive à les consulter[54].

---

pp. 35-36. Sur le système automatisé d'identification de numéros de plaques de véhicules (AFNES): RÉMY M., *Droit des mesures policières*, Genève/Zürich/Bâle, 2008, pp. 111-112. Le Tribunal fédéral s'est prononcé sur la durée de conservation d'enregistrements de vidéosurveillance sur des places et des voies publiques (ATF 133 I 77, Diggelmann, du 14 décembre 2006), sur l'utilisation à titre de preuves d'enregistrement vidéo obtenus de manière illicite en procédure pénale (ATF 131 I 272, X, du 3 mai 2005) et sur la surveillance vidéo d'un assuré par un détective privé pour le compte de l'assurance-accidents (135 I 169, N, du 15 juin 2009) ou de l'assurance privée RC et son utilisation ultérieure par la SUVA (ATF 129 V 323, F., du 25 février 2003 et 132 V 241, M., du 20 mars 2006).

52 Contrairement à ce que continuent de penser beaucoup d'utilisateurs, les données effacées d'un support informatique restent accessibles, ou à tout le moins des fragments importants.

53 BONDALLAZ S., *supra* note 49.

54 Sur la sécurité des données du point de vue de la protection des données, *cf.* la contribution de STAEGER A. dans le présent ouvrage.

4. Les moyens de limiter les risques créés par la surveillance

4.1 Les moyens juridiques

Le premier moyen est de disposer d'un cadre juridique clair et complet. C'est d'ailleurs une exigence constitutionnelle et conventionnelle que d'avoir une base légale accessible et suffisamment précise pour permettre au citoyen de prévoir les conséquences de son comportement. Le citoyen doit savoir à l'avance en quelles circonstances et sous quelles conditions les autorités publiques peuvent prendre des mesures secrètes[55].

Il faut ensuite disposer des moyens de contrôler le respect de ce cadre légal. Cela passe par un contrôle d'office avant que ne débute la surveillance: c'est la procédure d'autorisation. On parle de contrôle *a priori*. Le CPP prévoit une procédure basée sur celle de la LSCPT[56]. Le ministère public ordonne par exemple les mesures de surveillance de la correspondance par poste et télécommunication (art. 269 et 273 CPP) et l'utilisation d'autres dispositifs techniques de surveillance (art. 280 CPP). Ces mesures doivent ensuite être autorisées par le tribunal des mesures de contrainte (art. 274 CPP). La surveillance des relations bancaires est ordonnée par le tribunal des mesures de contrainte sur proposition du ministère public (art. 284 CPP).

---

[55] Les arrêts Calmanovici c. Roumanie du 1er juillet 2008, no 42250/02, et Dumitru Popescu c. Roumanie (N° 2) du 26 avril 2007, no 71525/01, confirment la jurisprudence rendue précédemment notamment dans les arrêts Klass c. Allemagne, du 6 septembre 1978, série A nº 28, Malone c. RoyaumeUni, du 2 août 1984, série A nº 82, et Kruslin c. France et Huvig c. France, du 24 avril 1990, série A nº 176-A et 176-B, Valenzuela Contreras c. Espagne, du 30 juillet 1998, Rec. 1998-V, p. 1910 et P.G. et J.H. c. Royaume-Uni du 25 septembre 2001, N° 44787/98, § 57, CEDH 2001-IX. Sur l'influence des arrêts Klass, Malone, Schenk, Huvig et Kruslin: VIENNE R., *«Les écoutes téléphoniques au regard de la Cour européenne des droits de l'homme»*, in: *Mélanges offerts à Georges Levasseur*, pp. 263-285, Paris 1992.

[56] *Cf.* notamment: BIEDERMANN A., *«Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000»*, Revue pénale suisse 2002, Vol. 120 (1), pp. 77-106; BONDALLAZ S., *La protection des personnes et de leurs données dans les télécommunications*, Zurich, 2007, pp. 507-522; HANSJAKOB, *supra* note 16; HAUSER R./SCHWERI E./HARTMANN K., *Schweizerisches Strafprozessrecht*, Bâle, 2005, pp. 358-366; OBERHOLZER N., *Grundzüge des Strafprozessrechts: dargestellt am Beispiel des Kantons St. Gallen*, Berne, 2005, pp. 555-565; PIQUEREZ G., *Traité de procédure pénale suisse*, Genève/Zurich, 2006, pp. 621-623; STRÄULI B., *«La surveillance de la correspondance par poste et télécommunication: aperçu du nouveau droit»*, in: U. Cassani/V. Dittmann/R. Maag, [*et al.*] (éds), *Mehr Sicherheit – weniger Freiheit? Ermittlungs- und Beweistechniken hinterfragt = Plus de sécurité – moins de liberté? Les techniques d'investigation et de preuve en question*, Zurich/Coire, 2003, pp. 140-153.

En plus de la procédure d'autorisation, à laquelle la personne surveillée ne peut pas prendre part puisque la mesure est le plus souvent secrète, on doit prévoir une procédure de contrôle *a posteriori*. C'est par le biais de cette procédure que la personne surveillée peut s'opposer, non pas à la surveillance puisqu'elle aura généralement déjà pris fin, mais à l'utilisation des résultats obtenus par cette surveillance. Ce recours contre la communication de la surveillance doit être formé devant l'autorité cantonale de recours[57]. Malheureusement, le Tribunal fédéral considère qu'un recours est irrecevable si il est déposé avant la réception de la communication de la surveillance faite par l'autorité à la personne surveillée[58]. La décision autorisant (ou refusant) la surveillance n'est pas susceptible de recours[59]. La personne surveillée ne peut pas solliciter un contrôle avant que l'autorité ne lui transmette la communication l'informant qu'elle a fait l'objet d'une surveillance et des droits en découlant, ce qui est regrettable.

Parallèlement à tout cela un contrôle strict des initiatives individuelles qui pourraient être prises pour contourner les procédures en place doit être prévu. C'est le cas par exemple avec les sanctions disciplinaires qui guettent les autorités policières.

4.2 Les moyens techniques

Les informaticiens ont pour habitude de dire que le point faible de l'ordinateur est l'utilisateur. Cette réflexion n'est pas dénuée d'un certain bon sens. Un grand nombre des risques pourraient être limités par une formation appropriée et une responsabilisation des personnes ayant accès à des données sensibles. La plupart des accès indus à des locaux ou des systèmes informatiques sont rendus possible parce que les machines ne sont pas mises à jour régulièrement, parce que les locaux sont trop facilement accessibles, ou encore parce que toute l'entreprise partage le même mot de passe qu'un employé a inscrit sur un post-it collé à son écran!

Des conditions de travail adéquates et des moyens techniques suffisant jouent également un rôle important. Mais une bonne infrastructure mal utilisée ne permettra jamais de limiter les risques.

---

57 En matière de surveillance de la correspondance (art. 279 al. 3 CPP), de surveillance des relations bancaires (art. 285 al. 4 CPP) et d'utilisation d'autres dispositifs techniques de surveillance (art. 279 al. 3 et. 281 al. 4 CPP).

58 ATF 1P.15/2003 du 14 février 2003, et HANSJAKOB, *supra* note 16. Si cette solution évite à l'autorité de recours de se prononcer lorsqu'une surveillance est en cours et d'indiquer au prévenu s'il fait ou non l'objet d'une surveillance, elle est problématique car elle l'empêche de faire valoir ses droits avant la fin de la surveillance, et ainsi avant la fin de l'atteinte qu'il estime injustifiée.

59 ATF 133 IV 182, 183-187, Ministère public de la Confédération, du 15 mars 2007.

5. Conclusion

La surveillance technique est tout à la fois un moyen réduire des risques existants qu'un élément générateur de risques. Souvent la surveillance, et en particulier la vidéosurveillance, est présentée comme la solution à tous les maux. Il est faux de suivre un raisonnement aussi simpliste. Les mesures de surveillance sont en revanche un élément positif, lorsqu'elles sont utilisées correctement et avec d'autres mesures (qui peuvent être des mesures policières dans le cadre d'une enquête ou des mesures éducatives, environnementales ou sociologiques dans le cadre de la lutte contre le sentiment d'insécurité).

Les risques générés par les mesures techniques de surveillance étatiques peuvent être fortement limités en soumettant ces mesures à un contrôle judiciaire indépendant *a priori* et en permettant ensuite à la personne surveillée de contester *a posteriori* la surveillance, également devant une autorité judiciaire indépendante. Il faut ensuite être conséquent et exclure toute utilisation des informations obtenues illégalement. Une formation technique suffisante des magistrats est encore essentielle, comme le fait de disposer du temps nécessaire à un examen correct des dossiers.

La situation en matière de surveillance privée est beaucoup plus inquiétante. L'ubiquité des données électroniques, l'internationalisation des réseaux informatiques et la multiplication des acteurs rend déjà la simple compréhension de la situation difficile. Il est ensuite presque impossible pour une personne seule de se battre contre des mesures de surveillance, même si elles sont illicites. Un cadre juridique devrait donc être établi rapidement et les violations de ces règles poursuivies d'office ou au moins également à l'initiative d'un organe étatique.