Maître Bensoussan répond à vos questions

Dans son dernier rapport rendu public en juillet, la Commission nationale de l'informatique et des libertés (CNIL) dresse le bilan complet de son activité en 2011. Du point de vue de la vidéoprotection, depuis la Loppsi2 du 14 mars 2011, la CNIL est désormais compétente pour contrôler les dispositifs installés aussi bien dans les lieux ouverts au public et sur la voie publique que dans les lieux non-ouverts au public. Et elle est la seule à pouvoir diligenter des contrôles sur les dispositifs de vidéoprotection et de vidéosurveillance sur l'ensemble du territoire national…

Avec 150 contrôles réalisés en 2011 (dont 25 % réalisés dans le secteur public), la CNIL a-t-elle les moyens de ses ambitions face aux 950 000 dispositifs installés sur l'ensemble du territoire national ?

Le niveau des contrôles a beaucoup évolué depuis leur institution. On peut distinguer trois périodes. Jusqu'à 2004, la priorité des contrôles et, de manière générale, la majorité de l'activité de la CNIL, était orientée vers le secteur public. De 2004 à mars 2011, une évolution importante a eu lieu avec le recentrage des contrôles de la Commission sur le secteur privé, si bien que 90 % des contrôles étaient réalisés dans ce secteur. Avec la Loppsi2 du 14 mars 2011, les nouvelles compétences en matière de vidéoprotection de la CNIL ont renforcé de nouveau son contrôle sur le secteur public et cette nouvelle approche me paraît intéressante. Je pense que, par ailleurs, la CNIL a compris qu'il fallait qu'elle s'approprie cette compétence renforcée de contrôle que lui confère la Loppsi2, notamment pour faire respecter les principes généraux de la loi "Informatique et libertés". L'action de la Commission est d'autant plus pertinente puisque, semble-t-il, la protection des libertés individuelles n'était pas forcément en ligne avec les exigences légales. La CNIL a donc une vocation "naturelle" à exercer des contrôles en matière de vidéoprotection dans l'intérêt du respect de la liberté privée et publique.

La CNIL a d'autant plus les moyens d'exercer ces contrôles que ses bureaux de contrôle se sont étendus et, parallèlement, elle a très fortement augmenté ses compétences en matière d'ingénierie informatique, que ce soit sur les nouvelles technologies informatiques classiques comme sur la sécurité. Jusqu'à 2011, le niveau d'exigence de la Commission, notamment lors des contrôles, était plutôt d'ordre juridique que technique. Aujourd'hui, nous sommes véritablement dans une période de très haut niveau technologique, avec des contrôles extrêmement pointus. Aujourd'hui la CNIL s'est dotée d'un bureau d'experts de très haut niveau. Ce service de l'expertise informatique s'est étoffé en même temps que son niveau d'exigence technique. Par exemple, sur la journalisation de la traçabilité des actions et des programmes, il existe des exigences de type "Informatique et libertés" qui sont davantage "informatiques" que "libertés" selon moi.

Le bilan montre que 30 % des contrôles la CNIL en matière de vidéoprotection ont révélé une absence d'autorisation ou de renouvellement de l'autorisation préfectorale. Ce bilan a-t-il de quoi inquiéter les élus ?

Je pense que la notion de formalités devrait évoluer vers un système beaucoup plus déclaratif. En fait, les personnes en charge des formalités les oublient très souvent et on peut se demander si ces aspects "administratifs" ont encore du sens. On voit bien qu'on ne pourra pas descendre en dessous d'un certain ratio : 30 % c'est à la fois beaucoup et peu. Il s'agit ici d'oublis techniques et non de fraudes. L'obligation de formalités est peut-être derrière nous. Ce qui est important, c'est de vérifier si l'ensemble des droits fondamentaux liés à la mise en place de caméras ont été respectés. Selon moi, il est beaucoup plus important d'informer les personnes sur leurs droits en matière de vidéoprotection que de faire sa déclaration à la CNIL. Par ailleurs, bien que, dans les deux cas, le niveau de sanction de l'infraction soit très élevé, on peut se demander si c'est raisonnable. Aujourd'hui, il faut savoir que le non-respect des formalités préalables auprès de la CNIL est passible de cinq ans d'emprisonnement et 300 000 euros d'amende (art. 226-16 du Code pénal). En revanche, le fait que 40 % des contrôles révèlent que l'information des personnes est inexistante prouve qu'il y a au moins 20 % des cas où l'information préalable des personnes n'a pas été faite, ce qui est beaucoup plus préoccupant parce que, dans une démocratie électronique, l'information des personnes est vraiment stratégique.

Effectivement, ce bilan a de quoi inquiéter les élus, parce que ce sont des manquements de condition de forme qui sont soumis à des sanctions pénales élevées, même si encore aujourd'hui les poursuites restent résiduelles et les sanctions purement formelles. Je crois qu'il serait temps de réviser les textes pour supprimer les formalités préalables et renforcer peut-être la protection des personnes, c'est là que se situe à mon avis le nouveau centre de gravité. Egalement, un autre point qui ressort du rapport est la mauvaise orientation des caméras. Le contrôle des caméras me paraît un élément essentiel de contrôle dans le cadre d'une démocratie électronique. Il faudrait amener les utilisateurs à avoir des processus de contrôle qualité. Et il faut remplacer un formalisme déclaratif vers un formalisme d'action.

Contrairement à la Commission départementale de vidéosurveillance (CDV), la CNIL exerce ses contrôles sur place. Cela ne risque-t-il pas, à terme, de porter préjudice aux compétences de la CDV qui ne se déplace jamais ?

Effectivement, la cour des comptes avait déjà souligné ce problème dans un rapport daté de juillet 2011 (NDLR : rapport sur l'organisation et le gestion des forces de sécurité publiques, juillet 2011 — p. 234). Le contrôle de la légalité qu'exerce la CDV n'est pas inintéressant, mais la pratique de la CNIL a toujours été une pratique de terrain. Nous sommes ici en présence de deux cultures différentes. La culture de la CNIL à ce niveau-là est à la fois une posture de politique "Informatique et libertés" et une posture de sanction "Informatique et libertés". Cela vient aussi du fait que la CNIL est une juridiction. C'est sûrement l'un des éléments qui devrait accélérer la mise en conformité réelle et non pas seulement formelle des systèmes de vidéoprotection. Depuis longtemps déjà, la CNIL réclamait, à juste titre, une compétence étendue en ce domaine, pour qu'à terme elle devienne l'organe déterminant ou le seul organe institutionnel de contrôle. En tout cas, aujourd'hui, elle en a la compétence, la pratique et l'expérience.

Je pense qu'un organe actif et de terrain est la meilleure façon de faire connaître et appliquer la loi plutôt que d'imposer des formalités. Il faut savoir que la vidéoprotection et la vidéosurveillance sont au cœur de l'équilibre entre sécurité et libertés. Et là, nous avons besoin d'un régulateur de contrôle et de sanction, comme l'est la CNIL, car dans ce domaine-là, même s'il n'y pas de fraude délibérée, le non-respect des lois peut être lourd de conséquences pour les libertés. Aux CDV de voir si elles souhaitent augmenter leur pouvoir ou si, au fond, une nouvelle clé de répartition peut être envisagée entre les CDV qui feront du contrôle de légalité formelle et la CNIL qui fera du contrôle de terrain. Il y a là un partage qui n'est peut-être pas inintéressant pour, à la fois maîtriser la conformité des systèmes et limiter les budgets.

La CNIL assure de plus en plus la promotion de bonnes pratiques pour sensibiliser les acteurs intéressés par l'installation de caméras de surveillance au respect des règles juridiques. Témoin, sa collaboration avec l'Association des maires de France. Qu'en pensez-vous ?

Maître Bensoussan répond à vos questions *(suite)*

En matière de contrôles, les moyens sont toujours insuffisants, et il faut trouver un point d'équilibre entre les risques encourus et les budgets consacrés. Dès le départ en 1978, la CNIL a toujours exercé une mission de pédagogie et de conseil. Et, jusqu'à aujourd'hui, tous les présidents ont toujours considéré que la posture "Informatique et libertés" était avant tout une posture de partage des valeurs avec les utilisateurs de l'informatique plus qu'une situation de gestion du risque et d'application de sanctions. La CNIL a toujours assuré une mission de conseil auprès des personnes et organismes qui mettent en œuvre des traitements ou envisagent de le faire.

Donc il n'est pas étonnant que lors de l'extension de sa compétence aux caméras de vidéoprotection, elle ait continué avec sa culture de diffusion des bonnes pratiques, de l'information et, ensuite, du contrôle et des sanctions.

La Cnil assure quatre grandes missions dans ce domaine-là :

- en termes de politique générale d'abord, elle définit les bonnes pratiques et ceci sous formes de conseils, de guides, de recommandations… Elle a toujours eu cette volonté de traduire la loi en actions positives ;

- sa politique de pédagogie passe également par les rencontres avec les acteurs. C'est-à-dire que la CNIL participe à des groupes de travaux, auditionne les acteurs afin d'être plus proche de leurs besoins, des conditions d'utilisation, pour parvenir davantage une régulation par la pédagogie qu'une régulation par la sanction ;

- son rôle de conseiller est très important. Les professionnels, mais aussi toutes les personnes concernées, peuvent solliciter l'avis de la CNIL. Il est de son ADN de prodiguer des conseils. Cet élément est davantage déterminant que la politique de contrôle, En mai 2012, elle s'est même dotée d'une Direction des Etudes, de l'Innovation et de la Prospective (DEIP) pour être au plus près de la compréhension des technologies et de leur utilisation sectorielle ;

- enfin, la politique de publication de la CNIL est également importante, notamment via son rapport annuel et la documentation sur son site Internet.

La collaboration de la CNIL avec l'Association des maires de France (AMF) sur les bonnes pratiques dans ce domaine a vraiment du sens. "Les 10 conseils pratiques en matière de vidéoprotection et de vidéosurveillance", disponibles sur les sites de l'AMF et de la CNIL, sont l'illustration même de cette politique de pédagogie face à des textes difficiles. Lorsque la réglementation se transforme en boîtes à outils, on peut se demander si c'est la réglementation qui n'est pas claire ou si c'est la boîte à outils qui va au-delà. Le seul problème que l'on peut se poser pour une démocratie c'est : "Faut-il traduire ce que dit le Parlement en boîte à outils ?" La loi ne devrait-elle pas être plutôt facilement compréhensible par tous ? Je suis toujours préoccupé par de tels outils qui expliquent le Droit. Heureusement, le fait d'utiliser aujourd'hui le terme de "vidéoprotection" versus "vidéosurveillance" permet de clarifier un peu les choses. Comme le terme de "technoprotection" qui traduit l'évolution des technosurveillances vers les technoprotections. Je suis d'ailleurs heureux de cette évolution terminologique que j'avais appelée de mes vœux.

Les chartes de déontologie et les comités d'éthique de la vidéoprotection sont très peu évoqués. Pourtant ne représentent-ils pas des outils qui permettraient aux collectivités de mieux remplir leurs obligations en matière d'information des personnes ?

Ma position est ici très claire. Les chartes de déontologie et comités d'éthique sont essentiels à la généralisation de la vidéoprotection. Je partage le sentiment qu'il faut des commissions de vidéoprotection pour un contrôle de la légalité qu'il soit formel ou réel. Je partage pleinement les pouvoirs de sanctions de la CNIL, notamment en matière de vidéoprotection, mais en tout état de cause il faut trouver un équilibre au plus près des citoyens entre l'exigence de sécurité et la protection de la vie privée. Cette exigence ne pourra jamais se limiter à un texte de loi, un décret, un arrêté… concernant les spécifications des caméras ou une liste de boîte à outils. C'est bien au plus près des zones où se trouvent ces caméras qu'il faut mettre le pouvoir. Car dans certaines zones d'insécurité, il faut installer des caméras ; dans d'autres, elles n'ont rien à y faire. De plus, ces zones évoluent avec l'urbanisation et la façon dont on met en place des plans de lutte contre l'insécurité…

Il me semble donc primordial de mettre en place des chartes éthiques. L'intérêt d'aborder la problématique par l'éthique est qu'elle est "infra morale" et "supra légale". C'est-à-dire qu'elle va permettre effectivement d'organiser la proportionnalité entre les exigences de sécurité et les libertés publiques où les éléments de la vie privée sont essentiels. Il me semble que la CNIL devrait encourager les comités d'éthique et les promouvoir. C'est la prise en compte d'une régulation de citoyenneté dans une démocratie numérique. On ne réglera pas ce principe de proportionnalité par des règles objectives. Ce n'est qu'en prenant compte la subjectivité des lieux, des rues en termes d'appréciation de la sécurité que l'on pourra trouver le bon équilibre entre sécurité et vie privée.

Le rapport de la CNIL constate que les fichiers d'antécédents judiciaires, Judex, Stic, ancien fichier des RG… sont erronés et peuvent conduire à de lourdes conséquences. La CNIL évalue à 1,3 million le nombre d'emplois concernés aujourd'hui par des procédures administratives. Quel recours peuvent avoir les victimes ?

Judex et Stic ont fusionné en mai 2012 pour devenir le traitement d'antécédents judiciaires. Ce fichier est nécessaire mais très préoccupant pour une démocratie car il a une incidence sur les enquêtes en cours et futures. Le fait d'avoir des instructions erronées est inacceptable. Il y a un travail des parquets, de la CNIL, mais d'abord et avant tout, des citoyens. La loi "Informatique et libertés" est une loi magnifique qui est devenue une référence pour l'Union européenne puisque 80 % de la directive communautaire sont issus de la loi française. Et c'est également un véritable processeur d'universalité puisqu'on ne peut exporter des données vers les pays tiers que si ces derniers ont une protection équivalente du moins suffisante, sinon il est obligatoire de mettre en place un mécanisme de contrat garantissant la protection des données qui sont exportées. Ce qui fait qu'après avoir exporté nos Droits de l'Homme historiques, nous exportons nos Droits de l'Homme numériques dans le monde entier.

Ce bilan positif doit néanmoins être contrebalancé. La loi "Informatique et libertés" a créé des droits fondamentaux pour le citoyen mais ce dernier n'a pas pris la mesure de l'importance de ses droits et encore moins de leur mise en œuvre. Cela constitue une grande défaillance dans la plupart des pays et, notamment, en France. La régulation de ces erreurs doit être à la charge des opérateurs mais aussi à la charge des citoyens qui doivent s'intéresser aux données les concernant. Lorsqu'une enquête est terminée ou lorsque les informations communiquées par un citoyen montrent qu'il n'a plus de raison d'être "fiché", il doit faire valoir ses droits au retrait de ces informations-là. Les fichiers d'antécédents judiciaires sont erronés du fait du travail des Hommes et de l'informatique., La qualité des données ne pèse pas uniquement sur les opérateurs mais sur chaque citoyen dans son devoir d'être le policier de ses propres données.

Lire aussi notre rubrique « Retour sur... »

Quand la CNIL dresse le bilan de son activité en 2011

Page 14