

Ligue  
des **droits de  
l'Homme**

FOUNDEE EN 1944



**MA VILLE**

*ma Vie,*

**JE LA VEUX...**

*libre &  
cybercitoyenne*

Il est fondamental de participer aux débats,  
de voter et faire voter.

C'est pourquoi la Ligue des droits de l'Homme (LDH)  
entend porter dans le débat public des valeurs et des  
propositions qui servent l'intérêt général dans les  
politiques publiques, éclairées de droits et de libertés  
posés de manière égale pour toutes et tous, aptes à aider  
à un renouveau démocratique, social et écologique.

**Au nom du « droit à la sécurité » ou de la lutte contre certaines fraudes, l'usage sans réserve des fichiers, de la vidéosurveillance, de la biométrie et des divers contrôles et traçages électroniques porte atteinte à la vie privée.**

### **Une société du soupçon généralisé**

Le développement continu du numérique, de ses capacités de stockage, de ses applications aux secteurs de la sécurité, comme à celui des services au public, modifie radicalement les termes de la vie collective. La multiplication de ces outils voudrait faire croire que ces technologies sont seules à même de garantir une société sûre et que le prix à payer est une transparence toujours plus grande : ceux qui n'ont rien à se reprocher n'ont rien à cacher et ne devraient donc pas craindre d'être filmés, tracés, identifiés à tout moment. Loin de construire des rapports apaisés, la « société de surveillance » qui se met en place construit une société du soupçon généralisé, où l'innocent risque fort d'être un coupable qui s'ignore, où chacun devient une menace pour l'autre.

### **Des technologies qui permettent le meilleur mais aussi le pire : les fichiers**

Les dangers des fichiers sont principalement liés à la quantité des données enregistrées, à la durée excessive de conservation, à l'élargissement et aux détournements de finalité par leur interconnexion, ou encore par le ciblage de certaines catégories de population.

De même, l'identification biométrique se banalise avec l'utilisation des empreintes digitales ou palmaires pour accéder à des services courants comme les cantines scolaires, les piscines, les bibliothèques.

L'accroissement de ces possibilités de contrôle électronique, de « traçage » avec la multiplication de « puces » de plus en plus perfectionnées sont de prétendues avancées non souhaitables dans la gestion d'une commune.

Certaines de ces technologies sont consacrées à cataloguer des populations comme vulnérables ou menaçantes. Chômeurs, personnes âgées, étrangers en situation irrégulière, mineurs, délinquants, élèves « décrocheurs » dans certains quartiers, autant de catégories qui sont aujourd'hui fichées en tant que telles.

La mise en œuvre du Règlement général sur la protection des données (RGPD), depuis mai 2018, est un début pour créer les conditions d'encadrement des fichiers.

Les communes doivent veiller à une application rigoureuse de la loi Informatique et Libertés modifiée par la mise en œuvre du RGPD qui impose de solides garanties pour le respect de la vie privée. Il appartient à toutes et tous de maintenir une forte vigilance quant à la multiplication et l'usage des fichiers gérés par leur commune.

### **La vidéosurveillance et la reconnaissance faciale**

Les systèmes de vidéosurveillance ont été multipliés par la volonté d'un nombre croissant de maires, encouragés par les gouvernements successifs, notamment par une participation importante de l'Etat aux frais d'installation. Mais les frais de fonctionnement et de gestion liés à ces systèmes sont des charges financières lourdes pour les budgets des communes. Par ailleurs, la mise en place de ces outils n'est que rarement précédée d'un large débat citoyen indispensable au bien-fondé de ces installations.

Les évaluations scientifiques officielles de la vidéosurveillance à l'étranger ou les études réalisées en France

par des sociologues montrent que la vidéosurveillance est peu efficace pour prévenir les délits. La baisse de la délinquance n'est que de 3 à 5 % si les installations ont été décidées après concertation avec la population et associées à des dispositifs humains de prévention. Malgré ces constats édifiants, les promesses de nouvelles installations sont innombrables.

### L'intelligence artificielle face à l'humain

Pour rendre plus puissante cette surveillance généralisée, des projets émergent visant à ajouter aux caméras de plus en plus perfectionnées des applications de reconnaissance faciale. Cette technologie qui utilise l'intelligence artificielle et des données biométriques (image numérisée du visage) est particulièrement invasive et déshumanisante car elle permet, par un contrôle invisible, la surveillance permanente de l'espace public et l'abolition de l'anonymat. Défendre ses libertés fondamentales conduit à l'interdiction de la reconnaissance faciale à usage sécuritaire. S'il peut porter atteinte à la vie privée, le numérique peut aussi être un atout dans l'exercice de la citoyenneté ou une atteinte au fonctionnement démocratique : ainsi le rôle joué par les réseaux sociaux et les algorithmes pour influencer certaines élections ou consultations ou pour le succès de certaines pétitions est incontestable. L'intelligence artificielle, s'appuyant sur l'ouverture des données publiques, utilisée à bon escient, peut permettre d'améliorer la gestion municipale de l'eau, des transports publics, des ouvertures de classes ou de crèches ou encore des travaux de voirie... mais elle peut aussi générer des discriminations.

### La dématérialisation des services source de discriminations

Le Conseil d'Etat a rappelé le 27 novembre 2019 que le fait d'accomplir des démarches par voie dématérialisée (par des applications internet sur ordinateur ou téléphone portable) doit rester une option pour les usagers du service public et non une obligation.

La dématérialisation des démarches administratives doit rester une possibilité offerte aux usagers des services au public, elle ne doit pas être une source de discriminations mais accompagner avec des moyens humains adaptés, les 23 % de personnes mal à l'aise avec l'outil numérique qui, souvent déjà exclues, renoncent aux démarches d'accès à leurs droits.

Pour le Défenseur des droits, « *Aucune organisation administrative, aucune évolution technologique ne peut être défendue si elle ne va pas dans le sens de l'amélioration des droits, pour tous et pour toutes* ». Une « dématérialisation raisonnée » peut au contraire rendre des services à toutes celles et tous ceux qui souhaitent entrer dans cette démarche, mais avec la garantie d'un service d'accueil avec des « humains » au service des personnes qui ne souhaitent pas ou ne peuvent pas l'utiliser.

Les technologies elles-mêmes ne sont pas en cause mais l'idée qu'il serait possible, en généralisant les outils de surveillance de construire une société du « risque zéro », conduit à faire accepter aux citoyennes et citoyens des restrictions des libertés et des atteintes lourdes à la vie privée, alors que la sécurité se construit par des pratiques sociales, des moyens humains, des systèmes de solidarité entre générations, territoires et catégories sociales.

Vivre en sécurité est un projet qui relève fondamentalement du politique et non du technologique.