UNE POPULATION MOINS SURVEILLÉE, UNE SURVEILLANCE MIEUX CONTRÔLÉE

Le fichage policier et la vidéosurveillance, développés au nom de la lutte contre la délinquance, paraissent aujourd'hui ne pouvoir trouver de limite. Outre que ce quadrillage toujours plus serré de la population est loin d'être aussi efficace que le prétendent les gardiens de la *doxa* sécuritaire, l'argument de l'efficacité fait peu de cas du principe démocratique selon lequel il ne doit être porté atteinte aux libertés qu'en cas de stricte nécessité. À titre d'exemple, si tous les nouveaux-nés étaient fichés génétiquement, il est probable qu'à terme le taux d'élucidation des infractions s'en trouverait augmenté ; mais serions-nous alors encore en démocratie ? Comme l'a indiqué la Cour européenne des droits de l'Homme dans un arrêt *S. et Marper c. Royaume-Uni* du 4 décembre 2008, « la protection offerte par l'article 8 de la Convention [aux termes duquel « toute personne a droit au respect de sa vie privée (...) »] serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part ».

Le premier problème est donc quantitatif : le peuple n'est-il pas sur-surveillé ? Depuis les rapports Batho-Bénisti de 2009 et 2011, qui recensaient près de soixante fichiers de police, l'ampleur du fichage n'a pas été réduite, au contraire. Outre que certains fichiers ont été créés en toute illégalité, l'existence de toutes ces bases de données est-elle vraiment nécessaire ? De même, le volume de ces fichiers est-il raisonnable ? Le nombre de personnes fichées au TAJ (Traitement des antécédents judiciaires, issu de la fusion du STIC et de JUDEX) était proche de 9,5 millions en 2015. En 1997, 889 755 personnes étaient enregistrées dans le FAED (Fichier automatisé des empreintes digitales), elles étaient plus de 5 millions en 2015. En quinze ans, le nombre de personnes inscrites au FNAEG (Fichier national automatisé des empreintes génétiques) est passé de 2 635 à environ 3,5 millions. Il importe de repenser la finalité de ces fichiers, de limiter drastiquement les possibilités d'interconnexions et de mettre un terme à leur dévoiement en définissant des critères d'inscription beaucoup plus stricts. Il est par exemple totalement injustifiable que des personnes mises hors de cause ou ayant fait l'objet d'un simple rappel à la loi puissent y être maintenues ou qu'une personne ayant commis des dégradations puisse être enregistrée au FNAEG pendant quarante ans et au TAJ pendant vingt ans. Il a fallu plus de deux années après la condamnation de la France par la CEDH pour que le régime du FAED soit revu par le décret du 2 décembre 2015. Les limitations apportées à ce fichier restent toutefois insuffisantes. Quant au FNAEG, il continue d'enfler sous l'effet de l'abondement systématique.

Si les fichiers ouvertement dédiés au fichage politique (tels EDVIGE et EDVIRSP) n'ont pas prospéré, leurs versions édulcorées demeurent sous la forme de PSAP (Prévention

des atteintes à la sécurité publique) et ESAP (Enquêtes administratives liées à la sécurité publique). Surtout, entre le fichier TES (Titres électroniques sécurisés) et le PNR-API (*Passenger name record*), le fichage de la population par ses trajets ou ses données biométriques continue de croître contre les avis des défenseurs des libertés. Quant à la vidéosurveillance, elle a suffisamment fait la preuve de son inefficacité en Grande-Bretagne pour cesser d'être considérée comme une panacée inoffensive en France. Des statistiques fiables doivent être communiquées pour connaître le nombre de caméras déployées dans l'espace public, y compris celles autorisées par le décret du 29 avril 2015 dans les commerces. Ce nombre devra ensuite être réduit, de manière à limiter cette surveillance aux seuls endroits où elle pourra être vraiment utile au vu d'études préalables et indépendantes. La réduction de la part de cette technique dans le Fonds interministériel de prévention de la délinquance (FIPD) devra se poursuivre. Il conviendra d'interdire aux entreprises privées d'installer une caméra sur la voie publique et d'encadrer très strictement l'utilisation des drones de surveillance. Leur nature impose qu'ils ne puissent être utilisés que sur autorisation préalable d'un juge.

Le deuxième problème, qualitatif, porte sur le contrôle de ces techniques de surveillance. À titre indicatif, la Commission nationale de l'informatique et des libertés (CNIL) continue à rapporter qu'une très grande majorité des fiches du TAJ sont erronées : la fusion STIC-JUDEX l'a d'ailleurs démontré. Il importe de renforcer sensiblement les capacités de contrôle de l'autorité judiciaire, mais aussi de la CNIL elle-même, qui doit retrouver un pouvoir d'avis conforme et dont la composition doit par ailleurs assurer une représentation pluraliste. Seule la loi doit pouvoir autoriser la création d'un fichier de police. Les recours et procédures d'effacement doivent être simplifiés.

Un troisième problème concerne les possibilités d'accès aux fichiers de police et l'utilisation qui peut en être faite. Il conviendra de restreindre drastiquement l'accès à ces bases de données afin qu'elles ne puissent être utilisées qu'à des fins d'enquête judiciaire. Il faudra pour cela revenir sur les textes autorisant massivement le Conseil national des activités privées de sécurité (CNAPS) et les services de renseignement à y avoir accès.

Plus généralement, une loi ambitieuse pour la protection de la vie privée devra être votée pour encadrer strictement l'utilisation publique et privée de certaines technologies porteuses de lourdes menaces pour les libertés telles que la géolocalisation et la biométrie, pour mettre la France en conformité avec la jurisprudence de la Cour de justice de l'Union européenne sur la protection des données.

Enfin, il importera de renforcer le contrôle sur les services de renseignement. La délégation parlementaire au renseignement devra poursuivre sa montée en puissance afin que des rapports étoffés soient publiés, sans cancellation massive au prétexte du secret défense. Les mécanismes de la loi renseignement devront

être revus : l'utilisation des techniques intrusives devra être très strictement encadrée. Une autorité juridictionnelle indépendante, le cas échéant composée de magistrats des ordres judiciaire et administratif, devra opérer un contrôle *a priori* systématique. Certaines techniques, relevant de la surveillance de masse (boîtes noires, *IMSI catcher*) devront être proscrites tandis que d'autres devront être revues quant à la durée de surveillance et de conservation des données. L'entourage ne devra pas pouvoir faire l'objet de ces techniques et les champs permettant de recourir aux technologies devront être restreints pour exclure ceux ayant trait à la défense des intérêts économiques, de la politique extérieure ou les atteintes à la paix publique, critères autorisant aujourd'hui la surveillance de militants.