

Un sentiment diffus de surveillance

Lors d'un contrôle d'identité, il est fréquent que des quidams s'entendent dire qu'ils sont déjà « connus » des services de police, parfois même lorsque leur casier judiciaire est vierge. À l'inverse, les personnes contrôlées n'ont souvent aucune connaissance des informations dont elles font l'objet et ne peuvent donc pas s'en défendre. Lors d'un simple contact avec les autorités, de nombreuses personnes sont ainsi « profilées » à leur insu et ont de fortes chances d'être discriminées dans leurs rapports avec celles-ci.

UNE PROLIFERATION DE BANQUES DE DONNÉES

L'origine des informations dont disposent les autorités policières s'explique, bien entendu, par le fait que celles-ci ont, à tout moment, la possibilité de consulter différentes bases de données dont la plus connue est la Banque de données Nationale Générale (ci-après « BNG »). Le type d'informations encodées est très varié, le critère étant « l'intérêt concret que cette information présente pour l'exécution des missions de police [...] »¹. C'est, en premier lieu, au fonctionnaire de police qui introduit les données dans cette banque de données de s'assurer de la pertinence de celles-ci et d'évaluer si elles sont proportionnelles au but poursuivi². D'après les chiffres disponibles – extrêmement opaques, puisque non publiés officiellement *in extenso* depuis 2008³ – le succès de cette banque de données est tel qu'une personne sur cinq en Belgique y serait inscrite⁴. En 2017, 2,2 millions de personnes y figureraient. Ce chiffre serait passé à trois millions en 2019⁵. Depuis les infractions COVID ce nombre a très probablement explosé.

Parallèlement et extrêmement critiquables en raison de leur opacité, les services de police peuvent créer des banques de données particulières pour « des besoins particuliers » « dans des circonstances spécifiques »⁶. Ainsi, une banque de données particulière a été créée pour énumérer les œuvres perdues ou volées et pouvoir y intégrer des photographies de celles-ci⁷. De même, la zone de police Bruxelles-Capitale-Ixelles dispose d'une « tagothèque » visant à répertorier et identifier les auteurs de graffitis ou tags apposés sur le territoire de la zone⁸. Ces banques de données sont extrêmement nombreuses : il en existerait plus de huit cents en 2017⁹. Aujourd'hui, selon Franck Schuermans, membre-conseiller de l'organe de contrôle, leur nombre serait passé à 1000. La police « connaît » ainsi pas mal de monde, qui, de manière asymétrique,

1 Directive commune MFO-3 du 14 juin 2002 des Ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative, *M.B.*, 18 juin 2002 (ci-après Directive commune MFO-3).

2 Art. M2, 2.3. de la directive commune MFO-3 du 14 juin 2002 des Ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative, *M.B.*, 18 juin 2002 (ci-après Directive commune MFO-3).

3 Les derniers chiffres publiés sont disponibles dans le Rapport annuel du Comité P, 2007, p. 36, disponible sur le site Internet du Comité P (<http://www.comitep.be>).

4 À cet égard, voy. BAILLY O., « La banque de données non gérée », *Medor*, 14 avril 2021, disponible sur <https://medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/episodes/bng-la-base-non-geree-15-quizz/?full=1>.

5 *Ibidem*.

6 Art. 44/11/3, §2 de la loi sur la fonction de police.

7 Exposé des motifs du projet de loi modifiant la loi sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. Parl.*, Ch., 2013-2014, n°53-3105/001, p. 7.

8 Rapport d'activité 2012 de la zone de police Bruxelles-Capitale - Ixelles.

9 Dans un avis du 31 mars 2017, le C.O.C en a analysé environ huit cent. Par souci de transparence, on peut regretter que ledit avis n'ait pas été publié, au moins partiellement ; celui-ci étant uniquement référencé dans l'avis n°009/2018 du 12 décembre 2018 concernant l'avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structure à deux niveaux, publié dans *Doc. Parl.*, Ch., 2018-2019, n°54-3697/003, p. 37 et suivants.

n'a aucun droit d'accès direct au contenu des informations emmagasinées. Ceci exclut, par conséquent, toute possibilité de débat contradictoire dans l'hypothèse où des policiers décident de tenir compte de ces obscures informations lors de la rédaction d'un procès-verbal, qui, par la suite, peut éventuellement être transmis à un Procureur ou un Juge d'Instruction dans le cadre de poursuites judiciaires. De manière plus insidieuse, des informations glanées – pouvant inclure des opinions politiques ou des tendances religieuses – peuvent potentiellement être prises en compte lors d'une simple visite de l'agent de quartier dans le cadre d'un souci de voisinage. Autant d'informations stockées sans en être jamais informé et sans possibilité d'y accéder.

À titre d'exemple, les services de police ont non seulement l'obligation d'y consigner les données relatives aux personnes condamnées pénalement mais également celles suspectées d'avoir commis une simple infraction administrative. Sont également fichées les personnes « *susceptibles* » de porter atteinte à des biens mobiliers et immobiliers ainsi que les membres de groupements « *susceptibles* » de troubler l'ordre public. En 2005, la police d'Anvers considérait comme « *extrémistes* » des organisations comme Gaia, la Ligue Humaniste, Indymedia, l'organisation pacifiste Vaka, le Bond Beter Leefmilieu, le Davidsfonds, le Parti du Travail de Belgique, Médecine Pour le Peuple, le Front Anti-Fasciste, et même Hare Krishna. Quid des membres de la Ligue des droits humains ? De Technoplice ? Découlent de tout ceci d'importants risques d'atteinte à la présomption d'innocence de personnes qui ne sont pourtant reconnues coupables d'aucune infraction. En vertu de la jurisprudence européenne, les suspects et les condamnés doivent pourtant nécessairement faire l'objet d'un traitement différencié. En effet, la Cour européenne est d'avis que si « *la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donnent pas l'impression de ne pas être considérés comme innocents* ».



SANS AUCUN DROIT (OU PRESQUE)

Cette collecte et conservation des données dans de multiples bases de données est susceptible de générer un sentiment diffus de surveillance qui s'en trouve renforcé eu égard à l'impossibilité pour les personnes concernées d'obtenir des informations sur le traitement de leurs données. En effet, le système belge n'impose pas aux autorités compétentes d'informer les personnes concernées du fait qu'elles font ou qu'elles ont fait l'objet d'un traitement de données à caractère personnel. Ce n'est donc que « par hasard » qu'une personne prend connaissance de son inscription dans une banque de données policière. En outre, pour accéder à ses données, la personne concernée doit s'adresser à l'organe de contrôle de l'information policière (COC) qui se limite systématiquement à indiquer qu'il a procédé aux vérifications nécessaires. Impossible donc de savoir si des données ont été corrigées, archivées ou supprimées. Partant, la personne concernée est également dans l'impossibilité d'exercer un recours juridictionnel puisqu'elle n'a aucune information sur le traitement de ses données et sur l'éventuelle inexactitude de celles-ci.



Comme le souligne l'Avocate Générale dans l'affaire C 333/22, arrêt rendu le 16 novembre 2023, par la Cour de Justice de l'Union européenne (ci-après CJUE) « *Dans de telles circonstances, la personne concernée risque d'être totalement privée d'une protection juridictionnelle effective, puisqu'elle ne sait pas qui est le responsable du traitement et que, même si elle le savait, elle n'aurait pas le droit de s'adresser directement à lui. En outre, elle ne peut pas contester l'action de l'Organe de contrôle de l'information policière. Il me semble que la personne concernée est confrontée à un système dans lequel « toutes les portes lui sont fermées », ce qui est contraire à la directive 2016/680.* ». En effet, eu égard au nombre très important de banques de données policières, même si le droit belge le permettait, la personne concernée ne peut s'adresser directement auprès des services de police, responsable du traitement, celui-ci pouvant s'avérer difficile à identifier.

C'est cette opacité qui vient d'être sanctionnée par la CJUE au terme de l'arrêt C333/22. Néanmoins, s'il paraissait clair que notre système n'était pas conforme aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne garantissant respectivement le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, on peut s'inquiéter de l'absence totale de réaction des autorités compétentes suite à la censure de la CJUE alors que les droits de millions de personnes continuent d'être violés que l'on ait, ou non, quelque chose à se reprocher.