La banque de données nationale générale

Dumortier, Franck

Published in:
Kairos

Publication date:
2016

Document Version
le PDF de l'éditeur

LA BANQUE DE DONNÉES NATIONALE GÉNÉRALE : L'ŒIL DE SAURON ?

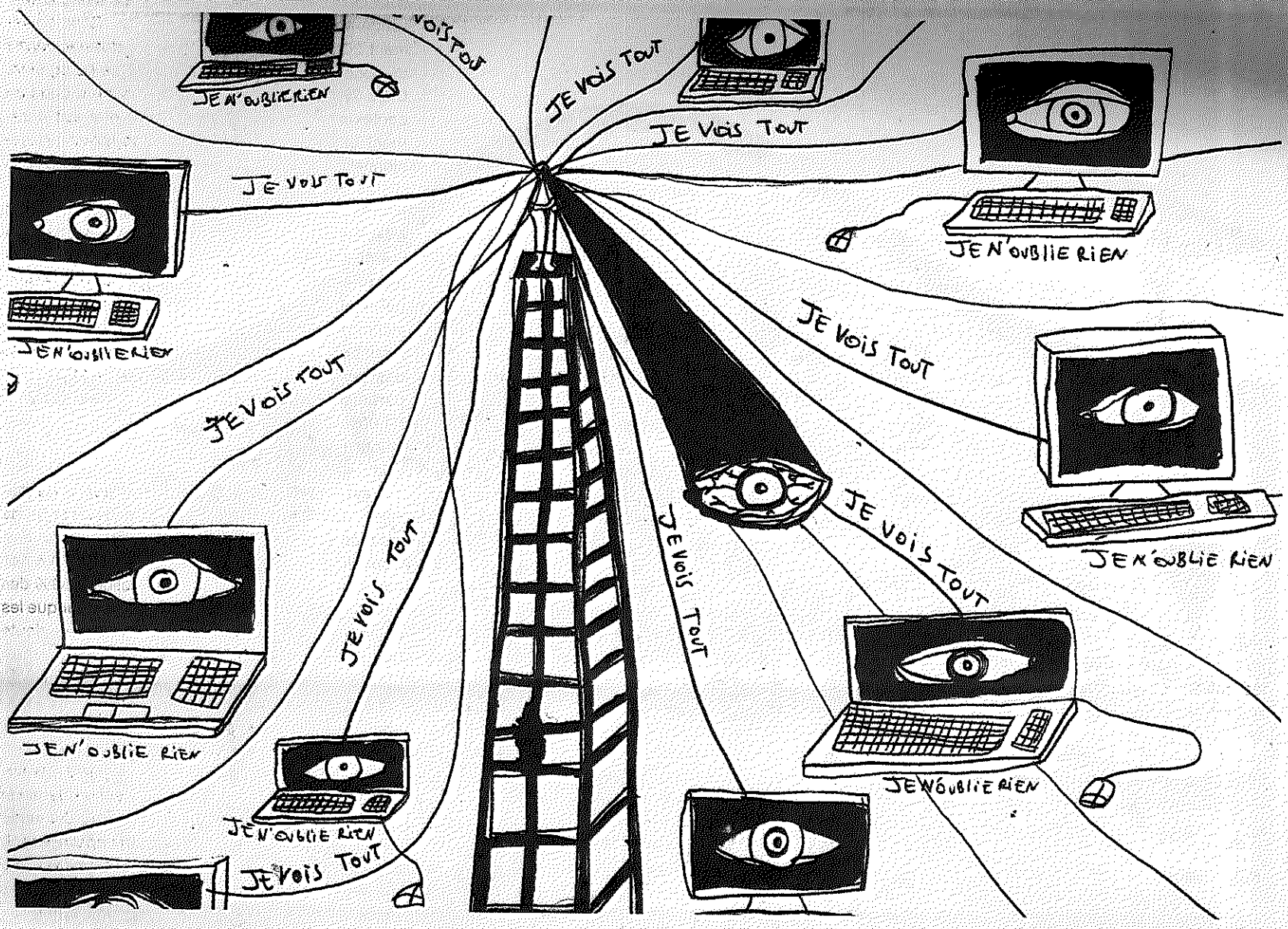

Illustration: Priscilla Beccari

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. A 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. L'origine des informations dont disposent les forces de l'ordre s'explique, bien entendu, par le fait que celles-ci ont, à tout moment, la possibilité de consulter une nébuleuse de bases de données dont la gestion est articulée autour de la Banque de données Nationale Générale (ci-après «BNG») qu'elles ont l'obligation d'alimenter au risque de poursuites pénales. D'après les chiffres disponibles – extrêmement opaques, puisque non publiés officiellement in extenso depuis 2008[1] – le succès du système est tel qu'il semble qu'une personne sur six en Belgique soit actuellement fichée. Au 31 décembre 2012, 1 769 439 personnes y figuraient. Afin de faciliter la collecte de données au sein de la BNG, un flux électronique a été mis en place afin que celle-ci soit alimentée par les données issues des procès-verbaux enregistrés dans des banques de données «de base»: FEEDIS (Feeding Information System) pour la police fédérale et ISLP (Integrated System for the Local Police) pour la police locale. En clair, la majorité des PV que la police rédige est intégrée dans la BNG, au moins de façon partielle.

La police «*connaît*» ainsi pas mal de monde, qui, de manière asymétrique, 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 encore plus insidieuse, des informations glanées à votre propos – pouvant inclure vos opinions politiques ou vos tendances religieuses – peuvent potentiellement être prises en compte lors d'une simple visite de l'agent de quartier dans le cadre d'un petit souci de voisinage. Dans le contexte sécuritaire en réponse aux attaques terroristes de Paris et de Bruxelles, la compilation, la conservation, l'utilisation et la communication par l'État de données à caractère personnel dans un fichier de police peut sembler légitime… Mais où placer la limite ?

LA POLICE A VOS DONNÉES. PAS VOUS !

Historiquement, c'est en 1998, suite à l'affaire Dutroux – et des nombreuses critiques qui s'ensuivirent sur les échanges d'informations défaillants –, que la BNG fut créée dans le but d'améliorer la circulation de l'information policière dans le pays. Depuis lors, la BNG rassemble une masse phénoménale de données relatives à des personnes identifiées ou identifiables… mais pas forcément coupables. La ministre de l'Intérieur avait beau tenter de nous assurer en 2013 que « *quand on est dans cette base, ce n'est pas pour des broutilles* »[2], un simple regard sur la loi suffit à convaincre qu'il n'est pas nécessaire d'être un délinquant pour y être enregistré. A 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

(1) Rapport annuel du Comité P 2007-2008.

(2) http://www.lavenir.net/cnt/dmf20131010_00372705.

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. Étant donné les perquisitions menées en 2014 dans le cadre des «emplois fictifs» dans le cabinet de l'Intérieur de l'Égalité des chances, il ne serait pas étonnant que Joëlle Milquet – pourtant porteuse du projet de réforme de la base de données policière – y soit référencée. En 2015, la Libre Belgique nous informait que les agents de police peuvent enregistrer, dans la BNG, les suspects ou auteurs de délits sous l'appellation «*tzigane*». Moi-même, ayant été candidat aux élections fédérales de 2007 au Parti communiste – erreur de jeunesse – et membre actif de la Ligue des Droits de l'Homme depuis de nombreuses années, j'y suis peut-être inscrit. Qui sait?

De la même manière que pour les adultes, l'inscription en BNG des mineurs âgés de 14 à 18 ans se fait sans l'intervention d'un quelconque magistrat. Aucune limite minimum n'est fixée pour l'inscription en BNG, en contradiction avec les Règles de Beijing et avec la Convention internationale des droits de l'enfant des Nations Unies. Dès lors, un enfant de n'importe quel âge peut être fiché en BNG: les errements de jeunesse sont impardonnables. Clairement, le projet de l'ancien président français N. Sarkozy de fichage dès la crèche est donc d'actualité... Pourtant, la Cour européenne des Droits de l'Homme a estimé que la conservation de données relatives à des personnes non condamnées pouvait être particulièrement préjudiciable dans le cas de mineurs en raison de leur situation spéciale et de l'importance que revêtent leur développement et leur intégration dans la société. Découle de tout ceci d'importants risques d'atteinte à la présomption d'innocence de personnes 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 donne pas l'impression de ne pas être considérés comme innocents*».

L'objectif de la BNG est évidemment de permettre l'identification des personnes susmentionnées, mais également de croiser ces données avec d'autres informations policières afin de vérifier leurs « *antécédents* » – très subjectifs, puisque non soumis à un contrôle judiciaire – dans le but d'aider les forces de l'ordre dans le cadre de leurs enquêtes et de savoir si des mesures à prendre sont prescrites vis-à-vis de personnes contrôlées (par exemple : fouille, contrôle approfondi, arrestation, saisie, audition, etc.). Les types de données collectées ne sont pas explicitement définies dans la loi et peuvent donc indistinctement consister en des noms, des adresses, des numéros de téléphone, des plaques minéralogiques, des photos, des enregistrements audiovisuels, voire des empreintes digitales ou des traces ADN sans parler des données politiques, syndicales, religieuses ou psychiques... De manière plus générale, peuvent être encodées n'importe quelles informations pour autant que celles-ci présentent un caractère «*adéquat*», «*pertinent*» et «*non-excessif*» pour la poursuite des crimes et délits (mission de police judiciaire) ou la prévention des atteintes à l'ordre public (mission de police administrative).

HASARDEUX ET DURABLE

En première ligne, c'est au policier qui introduit les données dans la BNG auquel revient la responsabilité d'évaluer si celles-ci sont proportionnelles au but poursuivi. A cet égard, il est piquant de relever que des informations fournies par des indicateurs ou par des citoyens déposant plainte – voire de simples rumeurs, dont celles véhiculées par le biais des réseaux sociaux – peuvent tout à fait être encodées dans la BNG dès lors qu'elles sont jugées intéressantes par le fonctionnaire en question. Dans son rapport annuel 2003, le Comité P (organe de contrôle des services de police) indique avoir constaté dans plusieurs dossiers que l'information obtenue est utilisée un peu trop à la légère: « *Dans un cas précis, il s'agissait d'une personne qui aurait été porteuse du virus du sida et aurait eu l'intention de contaminer les fonctionnaires de police lors d'une intervention policière éventuelle. Il est ressorti de l'enquête menée par le Comité Permanent P et par l'Organe de contrôle que l'information enregistrée reposait uniquement sur des rumeurs verbales, qu'il n'y avait aucune justification judiciaire ou administrative, que l'information reçue n'avait pas été évaluée de manière approfondie et qu'il n'y avait pas d'intérêt concret* ».

Outre le degré de qualité hasardeux des données intégrées dans la BNG, une autre préoccupation majeure découle des délais de conservation extrêmement longs prévus par la loi. Globalement, et sauf exceptions, les données relatives aux missions de police administrative sont accessibles aux fonctionnaires durant 5 ans à partir du jour de leur enregistrement et celles relatives aux missions de police judiciaire jusqu'à 15 ans s'il s'agit d'un fait qualifié de délit, 30 en cas de crime. Passé ces délais, ou lorsqu'elles ne sont plus considérées comme étant «*adéquates, pertinentes et non-excessives*», les données traitées en BNG ne sont pas *effacées* mais, au contraire, «*archivées*» pendant 30 ans, tant pour les personnes condamnées que pour celles simplement suspectées. Certes, durant la période « *d'archivage* », les données sont légalement consultables à des fins plus limitatives, il reste néanmoins que le citoyen est en droit de se demander si cette durée de rétention n'est pas contraire au prescrit selon lequel les données doivent être conservées « *pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées* ». Sur base de ce principe, la Cour européenne des Droits de l'Homme n'a d'ailleurs pas hésité à condamner l'État français alors qu'il prévoyait un délai de conservation de 25 ans, inférieur à celui prévu par la loi belge. L'inquiétude de voir les droits à l'oubli et au changement (!) violés est d'autant plus légitime lorsque l'on sait que rien ne prévoit la suppression automatique de données enregistrées dans le cadre d'un fait pour lequel une personne concernée est ensuite acquittée. Une communication vers les services de police est prévue mais, dans l'hypothèse où ceux-ci ne procéderaient pas à l'effacement qui s'impose, aucune voie de recours n'est ouverte aux citoyens. Il existe donc un risque de rester fiché par la police pour une infraction même si on a été acquitté pour ce fait par la justice.

Et ce n'est pas tout : qui dit collecte et enregistrement d'informations parle forcément de communication de celles-ci. Afin d'assurer un partage maximal d'informations, les données figurant dans les banques de données policières peuvent non seulement être consultées par les services de police belges mais également être communiquées à leurs homologues étrangers, aux autorités judiciaires, aux services de renseignements et de sécurité, au comité P, au comité R, à l'OCAM, à la Cellule de traitement des informations financières, à l'Administration générale des douanes et accises, à l'Office des étrangers, aux organisations internationales de coopération judiciaire et policière et aux services de répression internationaux (notamment Europol et Interpol). En outre, nos chers amis peuvent également consulter le Système d'Information Schengen, le SIS. Il a été créé pour compenser la suppression des contrôles aux frontières intérieures de l'espace Schengen.

En principe, ces autorités ne peuvent consulter la BNG que dans le cadre strict de l'exercice de leurs fonctions. Néanmoins, en 2005, le Comité P évoquait déjà « *un certain estompement de la norme* [qui] *régnerait au sein des services de police concernant l'utilisation des applications informatiques mises à leur disposition* ». Pour devoir constater encore dans son rapport annuel 2009 que « *certains membres de la police semblent continuer à abuser de leur accès à des données confidentielles à des fins personnelles* ». Par exemple, selon le quotidien De Morgen, au lendemain du suicide de la chanteuse flamande Yasmine en septembre 2009, plus de 900 policiers auraient consulté ses données. Étant donné la récurrence du phénomène, le Comité P a été amené une nouvelle fois à se pencher sur cette question en 2013 et à diligenter une enquête sur le sujet. Sur cette seule année, 1200 dossiers relatifs à des problèmes quant au respect de la vie privée étaient ouverts au comité P dont 126 comportant spécifiquement des allégations d'utilisation abusive de bases de données. Dans seulement 20,11% des cas, l'examen du dossier permit de conclure au caractère non établi de l'allégation. Dans 77,78% des cas, les faits se situent dans un contexte non professionnel, c'est-à-dire soit purement privé, soit en relation avec le milieu professionnel mais en dehors de l'exécution des missions de police. Paradoxalement, les flics se fliquent eux-mêmes. Les membres des services de police sont effectivement régulièrement l'objet des agissements illégitimes (18,25% des cas) : il s'agit essentiellement des collègues des membres du personnel impliqués. Les autres catégories importantes de victimes sont, par ordre décroissant d'importance : des personnes sans lien direct avec les membres des services de police concernés (14,29%) ; les partenaires, ex-partenaires ou relations de ceux-ci (11,90%) ; et les membres de la famille ou leurs relations (9,52%).

Il est enfin intéressant de relever que la découverte d'accès illégitimes découle davantage de plaintes externes adressées directement aux services de police, à l'AIG ou au Comité P (46,83% des cas) que de plaintes internes à la police (1,59% des cas). Cette information convaincra le lecteur que les chiffres publiés par le Comité P ne sont sans doute que la partie visible de l'iceberg, car pour porter plainte encore faut-il que le citoyen sache qu'il est fiché et que ses données ont été consultées de manière inappropriée... En Belgique, l'accès direct des citoyens aux données dont dispose la police n'est pas permis. Il faut, d'office, passer par l'intermédiaire de la Commission de la protection de la vie privée qui peut opérer ce contrôle, à la demande de la personne visée. C'est ce qu'on appelle le droit d'accès indirect. Pour ce faire, il faut envoyer une demande datée et signée à la Commission. Sous peine d'irrecevabilité, la demande doit contenir : nom, prénom, date de naissance, nationalité de la personne concernée, une photocopie de son document d'identité. Il faut aussi désigner l'autorité ou le service concerné et « *tous les éléments pertinents* ». En réponse, le demandeur n'aura, le plus souvent, pas d'autre information qu'un avis lui signalant que « *les vérifications nécessaires ont été effectuées* ». Il n'y a pas moyen d'être plus opaque.

J'ai bien conscience que cet article n'inspire pas l'espoir de vivre dans une démocratie vivante qui devrait, en principe, débattre de la mise en place d'un dispositif avant de le normaliser, surtout dans le contexte anti-terroriste actuel. Et j'en rajoute, malheureusement, en guise de conclusion: la BNG est régulée par voie législative seulement depuis mars 2014. Avant cette date, la BNG n'était encadrée que par le biais de circulaires ministérielles et de directives internes non consultables par le citoyen. Mais depuis lors, les statistiques relatives à son contenu sont inexistantes: la loi qui avait pour objet de rendre la BNG transparente a produit le résultat inverse. La Ligue des Droits de l'Homme et la Liga voor Mensenrechten ont décidé d'introduire un recours devant la Cour constitutionnelle contre la nouvelle loi sur la gestion de l'information policière. Croisons les doigts.

Franck Dumortier