De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme

Virginie Gautron, David Monniaux

De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme

Virginie Gautron, Maître de conférences en droit pénal et sciences criminelles, Laboratoire Droit et Changement Social, Université de Nantes

David Monniaux, Directeur de recherche au CNRS, Laboratoire VERIMAG

« *Depuis au moins l'époque de Fouché, la « police de l'ombre » n'a cessé de hanter l'imaginaire collectif (Dewerpe, 1994) : les agents et les indicateurs qui observent, surveillent, glanent et retranscrivent dans des dispositifs bureaucratiques de mémorisation des informations à l'insu de leurs cibles font partie de la mythologie politique de l'État moderne* »[1]. Si divers scandales, polémiques et mouvements de contestation populaires ont émaillé l'histoire des fichiers de police[2], ceux-ci ont au mieux conduit à une limitation du champ du fichage, jusqu'à ce que les attentats les plus récents aient raison de cette vigilance citoyenne, légitimant ce qui a de tout temps constitué un « *véritable savoir d'État […] mobilisé à des fins de contrôle social et de maintien de l'ordre* »[3]. Afin de transformer les agents de police en « *knowledge workers* »[4], de très nombreux traitements sont alimentés et consultés dans le cadre de la lutte contre le terrorisme[5], à des fins préventives comme répressives, au risque de générer des interférences, sinon une confusion croissante, entre les activités de police administrative et de police judiciaire[6].

Certains existent de longue date, même si leurs acronymes ont pu changer au fil du temps. Il en va ainsi du Traitement des Antécédents Judiciaires (TAJ), du Fichier Automatisé des Empreintes Digitales (FAED) et du Fichier National des Empreintes Génétiques (FNAEG), principalement réservés aux missions de police judiciaire[7]. Après que des parlementaires ont reconnu à demi-mot un accès des services de renseignement par des voies détournées[8], la loi n° 2015-912 du 24 juillet 2015 relative au renseignement a autorisé la consultation du TAJ pour certains services de renseignement dans le cadre de leur mission de prévention du terrorisme[9]. Dans un cadre initialement temporaire, mais pérennisé en 2014, ceux-ci peuvent également interroger le fichier national des immatriculations (FNI), les systèmes nationaux de gestion des permis de conduire (SI-FAETON), des cartes nationales d'identité (CNI), des passeports (TES) et des fichiers concernant plus spécifiquement les ressortissants étrangers

---

1 LINHARDT D., La « question informationnelle » éléments pour une sociologie politique des fichiers de police et de population en Allemagne et en France [années 1970 et 1980], *Déviance et Société*, 2005, Vol. 29, nº 3, p. 262

2 GAUTRON V., *Les fichiers de police*, Répertoire de droit pénal et de procédure pénale, Dalloz, 2015, n°2 et s.

3 PIAZZA P., « Violence symbolique et dispositifs étatiques d'identification », *in* CRETTIEZ X., MUCCHIELLI L. (dir.), *Les violences politiques en Europe*, 2010, La Découverte, p. 231

4 ERICSON R.V., HAGGERTY K. D., *Policing the risk society*, 1997, University of Toronto Press, p. 19

5 GARRIGOS-KERJAN M., « La tendance sécuritaire de la lutte contre le terrorisme. », *Archives de politique criminelle*, 2006, n° 28, pp. 187-213.

6 PARIZOT A., « Surveiller et prévenir... à quel prix ? Loi n°2015-912 du 24 juillet 2015 relative au renseignement », *JCP G*, 2015, 1077 ; HERRAN T., « La distinction entre police administrative et police judiciaire à l'aune de la loi relative au renseignement », *Law Review*, 2016, n°4.

7 GAUTRON V., *Les fichiers de police*, *op.cit*.

8 URVOAS J.-J., VERCHÈRE P., *Rapport d'information en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, n°1022, Assemblée Nationale, 2013, p. 28.

9 Art. L. 234-4 CSI, décret n°2015-1807 du 28 décembre 2015.

(AGDREF 2, VISABIO, GESI)[10]. Ils peuvent encore alimenter et consulter le Fichier des Personnes Recherchées (FPR), dont les finalités vont bien au-delà des missions de police judiciaire[11]. Les autorités administratives compétentes peuvent en effet demander l'inscription de personnes faisant l'objet de recherches « *pour prévenir des menaces graves pour la sécurité publique ou la sûreté de l'État, dès lors que des informations ou des indices réels ont été recueillis à leur égard* ». Le FPR comporte 21 types de fiches différenciant les motifs d'inscription, dont les désormais célèbres fiches « S », qui recensent les personnes potentiellement menaçantes pour la sûreté de l'État et dont le nombre oscillerait entre 5000 et 11000 selon les commentateurs, étant précisé qu'y figurent également des activistes, des militants politiques ou encore des hooligans. Malgré son obsolescence technique[12] et le fait qu'une simple suspicion policière puisse donne lieu à enregistrement, l'inscription des frères Kouachi, d'Amedy Coulibaly et de quelques autres a suffi à déclencher une succession de propositions politiques : expulsion de tout étranger suspecté d'islam radical et faisant l'objet d'une fiche « S », assignation à résidence, placement sous surveillance électronique voire dans des « centres d'internement ». Il faut encore ajouter des fichiers européens, dont le Système d'Information Schengen (SIS II)[13] qui stocke des données concernant plus d'un million de personnes[14], y compris aux seules fins de surveillance et de contrôle.

Ces dernières années, les pouvoirs publics n'ont cessé de multiplier les traitements de données plus spécifiquement dédiés au champ de la lutte anti-terroriste, essentiellement à destination des services de renseignement. Un seul de ces nouveaux fichiers est géré sous le contrôle de l'autorité judiciaire, même s'il tend lui aussi à effacer les frontières entre les missions de police judiciaire et de renseignement[15] : le Fichier Judiciaire des Auteurs d'Infractions Terroristes (FIJAIT)[16], introduit à l'occasion de la loi relative au renseignement sur le modèle du Fichier Judiciaire des Auteurs d'Infractions Sexuelles ou Violentes (FIJAISV). Les informations qui y sont collectées sont accessibles, pour une durée pouvant aller jusqu'à 20 ans, non seulement aux autorités judiciaires, aux officiers de police judiciaire et aux services de renseignement, mais aussi, indirectement et aux fins d'enquêtes de moralité, à de nombreuses administrations (préfectures, éducation nationale, PJJ, administration pénitentiaire, maires, etc.)[17]. Détailler le régime juridique applicable à ces différents fichiers n'aurait ici pas grand sens[18]. Cette contribution se concentre plus précisément sur deux évolutions majeures et problématiques. La première dévoile un véritable changement d'échelle, du fait de la généralisation de traitements ciblant potentiellement l'ensemble de la population, pour certains placés sous le sceau du secret (I). La seconde résulte d'innovations technologiques destinées, par le biais d'algorithmes prédictifs, à anticiper de potentiels mouvements terroristes (II). Toutes deux soulèvent de lourdes interrogations, tant sur le plan juridique, éthique, que pratique.

---

10 GAUTRON V., *Les fichiers de police*, *op. cit.*

11 Décret n°2010-569 du 28 mai 2010.

12 GAUTRON V., *Les fichiers de police*, *op. cit.* ; URVOAS J.-J., CAVARD C., *Rapport de la Commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés*, n° 1056, Assemblée nationale, 2013.

13 Art. R. 231-1 et s. CSI.

14 *Communication from the Commission to the European Parliament and the Council*, Overview of information management in the area of freedom, security and justice, 20 juillet 2010, COM(2010)385 final.

15 THOMAS-TAILLANDIER D., « Le nouveau fichier national des auteurs d'infractions terroristes », *AJ Pénal*, 2015, p. 523.

16 Art. 706-25-3 et s. CPP.

17 Art. 706-25-9 CPP, décret n°2015-1840 du 29 décembre 2015.

18 Pour une présentation détaillée de la règlementation applicable à la plupart des fichiers évoqués dans cet article, v. GAUTRON V., *Les fichiers de police*, *op. cit.*

I- Une extension du champ de la suspicion : vers une surveillance de masse

Bénéficiant d'une adhésion quasi-totale de la population, les pouvoirs publics ont introduit après chaque attentat de nouveaux fichiers, au point que ces annonces tendent à devenir un instrument de communication politique, à l'instar des lois pénales déclaratives qui se sont succédé au fil des faits divers. En l'absence d'oppositions citoyennes d'ampleur, ils ont multiplié les fichiers dont le contenu est maintenu secret (A), ainsi que des traitements visant potentiellement l'ensemble de la population (B).

A- La démultiplication des fichiers secrets

Les fichiers secrets sont loin d'être une nouveauté. Dès la création de la DST en 1944, son directeur, Roger Wybot, mit l'accent sur l'exploitation du renseignement en créant un service de documentation chargé d'exploiter les informations recueillies par les policiers sur le terrain pour identifier les résidents étrangers susceptibles de se livrer à des activités d'espionnage ou de terrorisme. A l'identique, les renseignements généraux ont constitué plusieurs bases de données, dont une application « violence-attentat-terrorisme », qui comprenait environ 60 000 références au début des années 1980[19]. Introduits sous une forme relativement artisanale, ces fichiers se sont considérablement développés sous l'effet de l'informatisation progressive des services de police. Si un décret n°86-326 du 7 mars 1986 permit *a minima* d'en connaître l'existence, le gouvernement eu recours aux dispositions de l'ancien article 20 al. 2 de la loi Informatique et Libertés du 6 janvier 1978 autorisant la dispense de publication des actes réglementaires relatifs aux traitements intéressant la sûreté de l'État. Seules les finalités, les personnes concernées et les données traitées par le Fichier Informatisé du Terrorisme mis en œuvre par les renseignements généraux furent publiées[20]. La direction centrale des renseignements généraux fut ainsi autorisée à mettre en œuvre ce traitement destiné à la « *centralisation des informations relatives aux personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'État ou à la sécurité publique par le recours ou le soutien actif apporté à la violence, ainsi qu'à celles entretenant ou ayant entretenu des relations directes et non fortuites avec ces personnes* ». Il enregistrait notamment des données relatives à l'état civil, l'adresse et la profession, ainsi que des éléments relatifs au « *signalement* », au « *comportement* », aux « *contacts* », aux « *déplacements* » et aux antécédents judiciaires des personnes. Les fichiers gérés par la Direction de la Surveillance du Territoire (DST), la Direction Générale de la Sécurité Extérieure (DGSE) et la Direction de la Protection et de la Sécurité de la Défense (DPSD) demeurèrent quant à eux secrets, ce que regretta la Commission Nationale Consultative des Droits de l'Homme (CNCDH)[21].

Depuis lors, les pouvoirs publics ont généreusement appliqué les dispositions de l'actuel article 26-III de la loi informatique et libertés autorisant l'absence de publication des textes réglementaires relatifs aux traitements intéressant la sûreté de l'État. Paradoxalement, les craintes populaires se sont cristallisées en 2009 sur la première version du fichier « EDVIGE », avec une pétition signée par plus de 100 000 personnes, alors que la publication

19 FRAYSSINET J., « Les décrets n° 91-1051 et 91-1052 du 14 octobre 1991 réglementant les fichiers et traitements automatisés des Renseignements généraux », *Recueil Dalloz*, 1992, p. 73.

20 Décret n°90-185 du 27 février 1990 modifié par le décret n°91-1052 du 14 octobre 1991.

21 Avis du 6 juin 1991 sur les nouveaux projets de décrets relatifs aux fichiers des renseignements généraux.

du décret avait *a minima* le mérite de la transparence[22]. En revanche, sa sœur « CRISTINA » s'imposa sans difficulté, pour reprendre et fusionner le fichier de la DST et certaines données des fichiers gérés par la Direction Centrale des Renseignements Généraux, dont le fichier informatisé du terrorisme. Comme pour les autres fichiers de la DGSE et de la Direction du Renseignement Militaire (DRM), listés à l'article 2 du décret n° 2007-914 du 15 mai 2007, nous ne connaissons de CRISTINA que la signification de son acronyme[23] et la mention d'un avis réservé de la CNIL. Depuis 2014, on compte également parmi ces fichiers secrets le nouveau Système d'Information de la Recherche et de l'EXploitation du renseignement de contre-ingérence (SIREX)[24], mis en œuvre par la DPSD, dont les missions recouvrent la lutte anti-terroriste, « *en alertant sur les vulnérabilités, renseignant sur les menaces potentielles, contribuant aux mesures de protection* ». En 2015 a été introduit le Fichier de traitement des Signalés pour la Prévention et la Radicalisation à caractère Terroriste (FSPRT)[25], qui contiendrait selon la presse plus de 11 400 fiches, dont les signalements recueillis par le biais du numéro vert et la plate-forme Internet anti-djihad. Il faut encore ajouter le fichier « CAR »[26], propre à l'administration pénitentiaire et destiné à la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique, qui pourrait contenir des informations sur des détenus radicalisés. Tous ont fait l'objet d'avis « avec réserve » de la CNIL.

B- Un changement d'échelle : le ciblage de l'ensemble de la population

Désormais, une bien plus forte proportion de la population se voit ciblée par des traitements dont les finalités portent sur la prévention et la répression du terrorisme. Autorisé par la loi n° 2006-64 du 23 janvier 2006 puis par un arrêté du 18 mai 2009, le traitement automatisé « LAPI » collecte à l'aide de dispositifs fixes ou mobiles les données signalétiques des véhicules, la photographie de leurs occupants, la date et l'heure de chaque photographie, ainsi que les coordonnées de géolocalisation[27]. Le droit français permet de collecter auprès des transporteurs aériens, maritimes, ferroviaires et routiers des données relatives à leurs passagers en cas de déplacements internationaux (art. L. 232-1 et s. et L. 232-7 et s. CSI ; art. L1631-4 Code des transports), notamment par le biais du fichier SETRADER[28] et du Système API-PNR France[29]. Ce dernier concerne l'ensemble des passagers des vols à destination et en provenance du territoire national, à l'exception des vols reliant deux points de la France métropolitaine, visant de la sorte près de 100 millions de personnes par an[30]. L'article R. 232-14 du Code de la sécurité intérieure (CSI) fixe la liste des informations collectées : date(s) du voyage, identité, nationalité, date de naissance, adresse, numéro de téléphone, adresse électronique, autres noms de voyageurs figurant dans le dossier passager et « *toute autre information* », à l'exception de données sensibles au sens de l'article 8 de la loi du 6 janvier 1978. Le traitement enregistre également les résultats issus de mises en relation avec le FPR, le Système d'Information Schengen (SIS), le Fichier des Objets et des Véhicules Signalés (FOVES), le Système Informatisé concourant au dispositif de Lutte Contre les Fraudes

22 Décret n°2009-1249 du 16 octobre 2009. Il sera remplacé par le fichier de la police nationale relatif à la prévention des atteintes à la sécurité publique (PASP, art. R. 236-11 et s. CSI) et le GISPAP de la gendarmerie nationale (articles R. 236-21 et s. CSI) ; GAUTRON V.,« Usages et mésusages des fichiers de police : la sécurité contre la sûreté ? », *A.J. Pénal*, n°6, juin 2010.

23 Centralisation du Renseignement Intérieur pour la Sécurité du Territoire et des Intérêts Nationaux.

24 Décret n°2014-957 du 20 août 2014.

25 Décret n°2015-252 du 4 mars 2015.

26 Décret n°2015-1465 du 10 novembre 2015.

27 CNIL, Délibération n°2009-146 du 26 février 2009.

28 Arrêté du 11 avril 2013, JO du 20 avril.

29 Art. R. 232-12 et s. CSI, décret n°2014-1095 du 26 septembre 2014.

30 CNIL, Délibération n°2014-308 du 17 juillet 2014.

(SILCF) et le Fichier des documents de voyage volés et perdus d'Interpol (base ASF-SLTD d'Interpol). Une fonctionnalité « de criblage » s'exécute automatiquement lors de l'arrivée de nouveaux flux de données en provenance des compagnies aériennes. En cas de « hit » positif, l'information est transmise au service qui a émis le signalement dans le FPR et au service chargé de la police générale sur la plateforme empruntée par le passager[31]. Outre les accords « PNR » (*Passenger Name Record*) conclus par l'Union européenne avec les États-Unis, l'Australie et le Canada[32], une proposition de directive de la Commission européenne vient d'aboutir après de lourdes pressions du Premier ministre et du ministre de l'Intérieur français suite aux derniers attentats parisiens. Malgré des avis critiques du service juridique du Conseil de l'Union européenne et du Groupe de l'article 29, qui réunit les autorités nationales chargées de la protection des données dans les États membres[33], les propres réserves du Parlement européen ne l'ont pas empêché d'adopter le texte en avril 2016[34].

Autorisé à titre temporaire par la loi n° 2006-64 du 23 janvier 2006, l'accès aux données de connexion des citoyens a également été pérennisé par la loi n° 2013-1168 de programmation militaire du 18 décembre 2013, puis largement étendu par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement (art. L. 851-1 à L. 851-7 CSI)[35]. Le Premier ministre peut désormais autoriser le recueil, auprès des opérateurs de communications électroniques, après avis de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) sauf urgence absolue, des « *informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques* ». Selon l'Article L. 851-2 du CSI, un recueil en temps réel peut être individuellement autorisé pour une durée de deux mois renouvelable et pour les seuls besoins de la prévention du terrorisme, au sujet de personnes préalablement identifiées « *comme présentant une menace* ». Nombreux sont les commentateurs ayant pointé le caractère extrêmement vague de ce critère, « *dont la mise en œuvre reposera vraisemblablement sur un diagnostic de dangerosité et un pronostic de passage à l'acte terroriste par définition aléatoires* »[36]. Dans les mêmes conditions, l'article L. 851-3 permet la mise en œuvre de traitements automatisés sur les réseaux des opérateurs de télécommunications, par le biais de dispositifs qualifiés de « boîtes noires »*, destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste »*. S'il n'est théoriquement pas prévu de recueillir par ce biais des données identifiant directement les personnes, cette détection de « *données susceptibles de caractériser l'existence d'une menace à caractère terroriste* » pourra être suivie d'une levée de l'anonymat.

Malgré l'interdiction d'accéder au contenu des échanges, les métadonnées permettent d'identifier, ne serait-ce qu'indirectement, « *les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* »[37]. Cette captation de métadonnées est donc quasiment aussi intrusive que la transcription

31 *Ibid.*
32 GAUTRON V., *Les fichiers de police*, *op. cit.*, n°100.
33 *Ibid*., n°101.
34 La proposition devra désormais être approuvée formellement par le Conseil. Une fois publiée au Journal officiel de l'UE, les États membres disposeront d'un délai de deux ans pour la transposer en droit national. Projet de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (première lecture) - Adoption de l'acte législatif (AL + D) = Déclaration**,** ST 7829 2016 ADD 1 - 2011/023 (OLP).
35 ROUSSEL G., « Le régime des techniques de renseignement », *A.J. Pénal*, 2015 p. 520.
36 Avis de l'Assemblée plénière de la CNCDH relatif au projet de loi sur le renseignement, 16 avril 2015, p. 7.

des échanges eux-mêmes[38], comme en témoigne la possibilité de lever l'anonymat sur la base de données qui sont en réalité « *pseudo-anonymes* »[39]. Comme bien d'autres[40], des chercheurs de l'Institut National de Recherche en Informatique et en Automatique (INRIA) ont souligné l'absence de technique d'anonymisation sûre, résistant « *de manière robuste au croisement des sources d'information* »[41]. L'absence de censure par le Conseil d'État et le Conseil constitutionnel n'exclut pas de s'interroger sur les risques d'une surveillance de masse, d'un « *glissement assumé de la réaction à l'anticipation, de la répression à la prévention (à la prédiction ?)* »[42].

II- Une révolution méthodologique : l'émergence d'algorithmes à visée prédictive

Au-delà de cette collecte massive de données, de nouvelles méthodes algorithmiques sont appelées à révolutionner les méthodes traditionnelles d'investigation et d'analyse des comportements, perçues comme subjectives, faillibles et donc imparfaites[43] (A). L'effet de fascination provoqué par l'objectivation statistique tend pourtant à éclipser les arguments de ceux qui démontrent tant leur piètre efficacité que divers effets contre-productifs, notamment le risque d'un profilage discriminatoire (B).

A- L'informatique en renfort de « *l'anticipation de la menace* »[44]

Autorisée pour le traitement des données relatives aux passagers aériens et des données de connexion, la prédiction algorithmique vise la détection de potentielles menaces, de « *signaux faibles* » qui « *s'entendent de tendances, de modus operandi, ou encore de traces qui risquent d'être illisibles ou non détectables isolément, mais qui, rapportées à un ensemble de personnes, mettent en évidence des occurrences révélatrices de certains comportements* »[45].

---

37 CJUE, gr. ch., 8 avr. 2014, aff. C-293/12 et aff. C-594/12, Digital Rights Ireland Ltd c/ Minister for Communications, Marine and Natural Resources et a., n° 27 : JurisData n° 2014-008774 ;

38 COMMISSIONER FOR HUMAN RIGHTS, *Positions on counter-terrorism and human rights protection*, CommDH/PositionPaper(2015)1, 5 juin 2015 ; GANDY O., « Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems », *Ethics and Information Technology*, 2010, vol. 12, n°1, pp. 29-42 ; SCHAUER F. F., *Profiles, probabilities and stereotypes*, Cambridge: Harvard University Press, 2003 ; LATOUR X., « La loi relative au renseignement : un État de surveillance ? », JCP A, 2015, 2286.

39 INRIA, *Éléments d'analyse technique du projet de loi relatif au renseignement*, Note du 30 avril 2015.

40 V. notamment KORFF D., GEORGES M., *Passenger Name Records, data mining & data protection: the need for strong safeguards*, The Consultative Comittee of the Convention for the protection of individuals with regard to automatic processing of personal data, 2015, p. 34.

41 INRIA, *op. cit*.

42 PARIZOT A., *op. cit.*

43 JOH E. E., « The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing », *Harvard Law & Policy Review*, 2016, vol. 10, pp. 15-42 ; JOH E. E., « Policing by Numbers: Big Data and the Fourth Amendment », *Washington Law Review*, 2014, vol. 89, pp. 35- 61 ; RICH M., « Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment », *University of Pennsylvania Law Review* (Forthcoming, 2016), En ligne : http://ssrn.com/abstract=2593795; FERGUSON A. G., « Big Data and Predictive Reasonable Suspicion, *University of Pennsylvania Law Review*, 2015, vol. 163, pp. 328- 352 ; LATOUR X., « La loi relative au renseignement : un État de surveillance ? », *JCP A*, 2015, 2286.

44 Etude d'impact de la loi relative au renseignement, NOR : PRMX1504410L/Bleue-1, 18 mars 2015

45 CNIL, Délibération n° 2015-078 du 5 mars 2015, p. 9.

Le Système API-PNR France permet ainsi le ciblage d'individus grâce à l'utilisation d'un outil de *scoring* et d'une échelle de risque dont les critères demeurent inconnus[46]. A l'identique, l'étude d'impact de la loi relative au renseignement précise que les fameuses « boîtes noires » ont pour objet « *l'anticipation de la menace* », qui nécessiterait non seulement « *un suivi exhaustif des activistes déjà identifiés et répertoriés* », mais aussi « *la détection de personnes qui ne l'avaient pas été précédemment et qui se trouvent engagées dans des entreprises radicales aux fins d'anticiper leur éventuel passage à l'acte […]. Afin d'identifier le plus en amont possible l'existence de ces menaces, les services de renseignement, confrontés à une multitude sans cesse croissante de réseaux, modes et supports de communications générant au plan planétaire des flux massifs de données, doivent pouvoir recueillir, traiter, analyser et recouper un grand nombre d'éléments techniques anonymes pour détecter les signaux de faible intensité qui témoignent d'une menace pesant sur les intérêts de notre pays* ».

Ces nouveaux outils de renseignement sont chargés d'identifier des cas « suspects » sur la base d'un *algorithme*, autrement dit d'un calcul. Dans les approches les plus simples, on attribue un score à diverses caractéristiques, les concepteurs du système choisissant les caractéristiques pertinentes et la façon de leur attribuer ce score. Ces paramètres étant tenus secrets, il est impossible de débattre de leur adéquation et de leur éventuel caractère discriminatoire. Les récents débats sur les algorithmes ont plutôt porté sur les approches par *apprentissage automatique* (*machine learning*), où une part plus ou moins grande des paramètres de l'analyse est réglée automatiquement par l'algorithme lui-même, soit sur la base d'un corpus d'exemples des diverses catégories de cas à distinguer (*apprentissage supervisé*), soit de façon autonome (*apprentissage non supervisé*). D'importantes recherches, tant théoriques qu'appliquées, ont été menées sur le sujet, la représentation des données en entrée de l'algorithme d'apprentissage, le choix de l'algorithme d'apprentissage lui-même et de ses paramètres internes dépendent des représentations de leurs concepteurs, qui doivent non seulement parfaitement connaître ces méthodes, mais aussi le champ investigué[47]. Le choix du modèle d'analyse informatique et des variables mobilisées étant étroitement tributaire de leurs représentations sur ce qui est pertinent et sur la forme des relations à découvrir, l'impression d'objectivité masque potentiellement de simples interprétations subjectives et discrétionnaires, des jugements normatifs sinon des préjugés, avec des conséquences profondes sur le résultat final[48]. Il peut être très difficile, même pour ses concepteurs, de comprendre les choix opérés par un système basé sur l'apprentissage automatique, d'autant plus que le modèle d'apprentissage est complexe. Ces choix peuvent diverger de ce que les utilisateurs auraient attendu ou désiré. Enfin, un apprentissage mal mené peut produire un modèle non pertinent (par exemple, par des phénomènes de *surapprentissage*) : le contrôle de sa qualité est une affaire de spécialistes.

46 CNIL, Délibération n° 2014-308 du 17 juillet 2014.

47 Par exemple, les concepteurs des moteurs de recherche en ligne ont considéré qu'il est pertinent au premier abord d'analyser les documents par leur vocabulaire et la fréquence des différents mots, sans se préoccuper de leur ordre dans le texte.

48 JOH E. E., « The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing », *op.cit.*

B- Des effets contre-productifs

Nombreux sont ceux qui dénoncent le risque d'un profilage discriminatoire, ce dont s'est récemment inquiété le Commissaire aux droits de l'homme du Conseil de l'Europe[49]. Les variables sélectionnées par l'algorithme peuvent en effet fort bien aller à l'encontre du droit ou de la morale, perpétuer et renforcer les inégalités sociales[50]. Certes, les promoteurs de telles méthodes insistent au contraire sur l'effet de neutralisation des stéréotypes ethno-raciaux, biais implicites et interprétations subjectives des enquêteurs[51]. Sous certaines réserves, la législation française et internationale prohibe par ailleurs l'utilisation de données sensibles directement révélatrices de l'origine, des opinions politiques, religieuses, etc. Il n'en demeure pas moins que les algorithmes d'apprentissage sont susceptibles de mobiliser des critères largement équivalents à l'appartenance à un groupe social, culturel, religieux ou ethnique, par corrélations avec d'autres données, sans que leurs concepteurs en soient toujours conscients[52]. À l'instar des échelles actuarielles de prédiction des risques de récidive[53] et des applications cartographiques qui commencent à se déployer en France sur le modèle du logiciel américain « PredPol »[54], ces algorithmes pourraient confirmer le mécanisme bien connu de la prophétie auto-réalisatrice, la prise de décision renforçant pour la suite les biais initiaux, au risque de marginaliser et de stigmatiser des groupes entiers de population[55]. Institutionnaliser ces nouvelles pratiques décisionnelles aurait dès lors mérité de véritables réflexions et débats éthiques, la technologie n'étant ici, comme souvent, pas neutre. Sans doute les pouvoirs publics auraient-ils pu réinterroger les fondements de l'introduction en 1978 de l'article 10 de la loi Informatique et Libertés, selon lequel aucune décision « *produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ».

Ces dérives semblent d'autant plus problématiques qu'elles ne sont guère contrebalancées par des preuves de l'efficacité de tels dispositifs. De nombreux travaux insistent sur le caractère

---

49 « *These technologies suffer from built-in biases which lead to actions against large numbers of innocent people – and, in the anti-terrorist context, often risk discriminating on grounds of race, gender, religion or nationality* », COMMISSIONER FOR HUMAN RIGHTS, *op. cit.* ; GANDY O., « Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems », *Ethics and Information Technology*, 2010, vol. 12, n°1, pp. 29-42 ; SCHAUER F. F., *Profiles, probabilities and stereotypes*, Cambridge: Harvard University Press, 2003.

50 GANDY O. H., « Data mining, surveillance, and discrimination in the post-9/11 environment », in Haggerty K., Ericson R. (Eds.), *The new politics of surveillance and visibility*, University of Toronto Press, 2006, pp. 363-384 ; GANDY, O. H., BARUH L., « Racial profiling: They said it was against the law! », *University of Ottawa Law & Technology Journal*, 2006, vol. 3, pp. 297-327 ; GANDY O. H., « Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage, Ashgate, 2009, p. 55 ; GUZIK K., « Discrimination by Design: predictive data mining as security practice in the United States « war on terrorism » ; *Surveillance and Society*, 2009, vol. 7, n°1, pp. 3-20.

51 JOH E. E., « The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing », *op. cit.* ; FERGUSON A. G., « Big Data and Predictive Reasonable Suspicion, *op.cit*.

52 KORFF D., GEORGES M., *op. cit.*, p 36.

53 DUBOURG E., GAUTRON V., « La rationalisation des méthodes d'évaluation des risques de récidive », *Champ pénal/Penal field* [En ligne], Vol. XI | 2014, mis en ligne le 18 novembre 2014. URL : http://champpenal.revues.org/8947

54 BENBOUZID B., « De la prévention situationnelle au *predictive policing* », *Champ pénal/Penal field* [En ligne], Vol. XII | 2015, mis en ligne le 09 juin 2015, URL : http://champpenal.revues.org/9050.

55 « *It is especially in such dynamic systems that the risk of reinforcing engrained biases is greatest: feedback loops have a tendency to amplify such biases. Yet again, the very complexity of the algorithm tends to mask such effects: many users will not be able to detect such discrimination, or may be uninterested in it as long as the systems work to their benefit* ». KORFF D., GEORGES M., *op. cit.*, p. 28.

non seulement inopérant mais contre-productif de tels outils[56], notamment en raison des difficultés de détection des cas rares[57]. Lors des débats engagés au sujet de la loi relative au renseignement, les chercheurs de l'INRIA ont attiré l'attention sur « *le paradoxe des faux-positifs* ». Si l'on considère un algorithme présentant une marge d'erreur de 1%, ce qui est particulièrement faible, « *l'algorithme identifiera quelques 600 000 personnes sur une population totale de 60 millions de personnes. Si le nombre de vrais terroristes est par exemple de 60, ces vrais terroristes ne représenteront que 0,01% de la population identifiée »*[58]. Cette méthode automatisée de détection d'une criminalité rare, même fiable à 99,99 %, aboutirait dès lors à surveiller une écrasante majorité d'innocents. Il faut ajouter que les modes opératoires des terroristes varient et évoluent dans le temps, alors que les méthodes algorithmiques procèdent par induction à partir d'un passé connu, de sorte que Grégoire Chamayou, citant le juriste américain Jeffrey Rosen, considère que cela reviendrait à *«chercher une aiguille dans une botte de foin alors que la couleur et la forme de l'aiguille ne cessent de changer»*[59]. D'où le scepticisme de certains chercheurs en informatique à l'égard des prétentions du gouvernement de détecter automatiquement les profils à risque de radicalisation au vu de leurs communications. Une recherche aussi peu ciblée induit une multiplication des signalements que les forces de l'ordre ne seront pas en mesure de traiter, ceux-ci étant déjà dans l'incapacité de suivre l'ensemble des personnes déjà signalées ou fichées, ce qu'ont démontré les attentats les plus récents. Comme ont pu en témoigner des analystes de la NSA américaine, ce dispositif noiera les professionnels sous des masses d'informations[60]. Il engendrera des vérifications coûteuses qui ne donneront rien dans l'immense majorité des cas. À tel point qu'en 2015, le rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique recommandait d'interdire l'usage de cette technique de prédiction algorithmique, « *dont l'inefficacité a été prouvée dans les pays qui l'ont utilisée* »[61]. Un autre rapport a pointé les mêmes constats s'agissant des PNR[62]. Selon le chercheur Ian Brown, cette rétention de données pourrait au mieux permettre d'augmenter le taux d'élucidation de 0.002%[63]. Ces piètres résultats se font pourtant au prix de lourdes atteintes au respect de la vie privée et au droit à la sûreté, tant les méthodes algorithmiques contiennent le risque d'une intensification sans limite de la surveillance des opinions politiques et affiliations religieuses des citoyens. Cette surveillance de masse pourrait plus globalement avoir des effets délétères sur le plan de l'expression démocratique des idées, particulièrement des positions minoritaires[64].

---

56 « *Automated identification of terrorists through data mining (or any other known methodology) is neither feasible as an objective nor desirable as a goal of technology development efforts* », NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, 2008, p. 78.

57 KORFF D., GEORGES M., *op. cit.*, p.25.

58 INRIA, *op. cit.*, p. 3 ; v. également FERGUSON A. G., *op. cit.*

59 CHAMAYOU G., « Loi sur le renseignement : les bugs du big data », Libération, 14 avril 2015.

60 Amicus curiæ transmis au Conseil constitutionnel dans le cadre des saisines visant la « loi relative au renseignement », 25 juin 2015 ; MASS P., « Inside NSA, Officials Privately Criticize "Collect It All" Surveillance », The Intercept, 28 mai 2015.

61 PAUL V. C., FÉRAL-SCHUHL C., *Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique*, Assemblée nationale 2015, p. 155.

62 OMTZIGT P., *Mass surveillance*, Committee on Legal Affairs and Human Rights, Parliamentary Assembly, janv. 2015.

63 BROWN I., Communications Data Retention in en Evolving Internet, *International Journal of Law and Information Technology, 2010, vol. 19, n°2, pp. 95-109 ;* BROWN I., KORFF D., « Terrorism and the Proportionality of Internet Surveillance », *European Journal of Criminology*, 2009, vol. 6, n°2, pp. 119-135.

64 STOYCHEFF E., « Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring », *Journalism & Mass Communication Quarterly*, 2016, pp. 1-16.

Conclusion

Malgré les nombreux risques de dérapage évoqués, de sérieux doutes existent quant à la possibilité d'exercer un contrôle effectif des usages et des effets de ces nouveaux traitements de données. Certains fichiers secrets ne sont pas placés sous la surveillance de la CNIL, l'article 44 IV de la loi Informatique et Libertés la privant de tout contrôle sur place, de son droit d'accéder aux programmes informatiques et aux données. Son manque de moyens l'empêche par ailleurs de répondre aux demandes d'accès indirect dans les délais prévus par les textes, le délai moyen d'instruction des demandes étant de l'ordre de dix-huit mois lorsqu'une personne figure dans un fichier de renseignement[65]. A l'identique, et même si le Conseil constitutionnel et le Conseil d'État n'y ont pas vu matière à censure, de nombreux commentateurs ont souligné les pouvoirs limités de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR), dont les avis peuvent être écartés par le Premier ministre[66]. Les citoyens injustement ciblés pourront quant à eux difficilement contester les décisions prises sur la base de ces algorithmes et attester de leur bonne foi. Au-delà d'une délicate compréhension des modèles mathématiques en cause, les plaignants se verront rétorquer qu'ils sont placés sous le sceau du secret national voire commercial, au risque de sérieuses atteintes au procès équitable[67]. L'exercice des droits de la défense sera d'autant plus complexe que la loi relative au renseignement aménage de véritables atteintes au principe du contradictoire. Si le nouvel article L. 773-8 du Code de justice administrative engage un plus large accès du Conseil d'État aux fichiers de renseignement, il dispose que la formation de jugement se fonde sur les données mémorisées « *sans les révéler ni révéler si le requérant figure ou non dans le traitement* ». Sans « *faire état d'aucun élément protégé par le secret de la défense nationale* », elle l'informera de la conservation de données « *inexactes, incomplètes, équivoques ou périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite* ». Toutefois, la rectification, suppression ou mise à jour demeure une simple faculté pour la formation de jugement.

La propension des pouvoirs publics, parfois des juridictions nationales, à occulter la jurisprudence de la Cour Européenne des Droits de l'Homme (CEDH) et de la Cour de Justice de l'Union Européenne (CJUE) n'est pas moins inquiétante. Quand bien même leurs arrêts ne viseraient pas directement la France, nombre d'entre eux soulèvent des interrogations quant à la conventionnalité de la réglementation française. La conformité des fichiers relatifs aux passagers aériens et aux données de connexion pose question au regard des analyses développées par la CJUE dans son arrêt « Digital Rights » du 8 avril 2014 [68]. La jurisprudence de la Cour EDH sur les fichiers secrets est particulièrement claire[69], mais n'est curieusement jamais évoquée en France, dont les autorités pensent peut-être qu'il n'y a pas d'urgence tant qu'elle n'est pas elle-même condamnée. La Cour a notamment considéré que le fait de conserver des données dans un fichier créé par un arrêté qui n'a fait l'objet d'aucune publication et n'a pas été rendu accessible au public constitue une violation du droit au respect

65 CNIL, Guide Droit d'accès, éd. 2010, p. 10.

66 LAZERGES C., HENRION-STOFFEL H., Politique criminelle, renseignement et droits de l'homme. A propos de la loi du 24 juillet 2015 relative au renseignement, RSC 2015 p.761 ; PARIZOT R., op. cit. ; LATOUR X., op. cit.

67 « *It is extremely difficult to provide for serious accountability in relation to, and redress against, algorithm-based decisions generally* », KORFF D., GEORGES M., *op. cit.*, p. 30. ; v. également CITRON D. K., « Technological Due Process », *Washington University Law Review*, 2007, Vol. 85, pp. 1249-1313.

68 CJUE, 8 avr. 2014, Aff. C-293/12 et C-594/12, Digital Rights Ireland Ltd & Michael Seitlinger e.a. ; GAUTRON V., *Les fichiers de police*, *op. cit.*, n°102 et s.

69 V. notamment CEDH, 21 juin 2011 req. nº 30194/09, Shimovolos c/ Russie ; CEDH, 10 févr. 2011, req. nº 11379/03, Dimitrov-Kazakov c/ Bulgarie ; GAUTRON V., *Les fichiers de police*, *op. cit.*, n°82 et s.

à la vie privée[70]. L'exigence de prévisibilité est selon elle d'autant plus nécessaire concernant les fichiers de renseignement impliquant une surveillance secrète. En effet, « *le danger d'arbitraire apparaît avec une netteté singulière là où […] un pouvoir de l'exécutif s'exerce en secret. Puisque l'application de mesures de surveillance secrète échappe au contrôle des intéressés comme du public, la "loi" irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire* »[71]. Certes, la Cour admet des restrictions concernant les activités touchant à la sécurité nationale, car « *l'exigence de prévisibilité ne saurait cependant être la même qu'en maints autres domaines. Ainsi, elle ne saurait signifier qu'un individu doit se trouver en mesure d'escompter avec précision les vérifications auxquelles la police […] procédera à son sujet en s'efforçant de protéger la sécurité nationale. Néanmoins, […] la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée* »[72]. De sorte qu'il y a violation de l'article 8 lorsque la norme interne ne définit « *ni le genre d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre* »[73]. Ces précautions démocratiques ont systématiquement été écartées lors des réformes les plus récentes de la réglementation française. Dans un contexte international qui tend de plus en plus à les disqualifier, ces deux juridictions européennes seront sans doute, selon leur capacité de résistance aux pressions politiques et citoyennes, les seules à même de protéger notre État de droit de telles dérives autoritaires.

70 CEDH, 21 juin 2011 req. nº 30194/09, Shimovolos c/ Russie.

71 CEDH, 6 juin 2006, req. nº 62332/00, Segerstedt-Wiberg c/ Suède, §76 ; CEDH, 4 mai 2000, req. nº 28341/95, Rotaru c/ Roumanie.

72 CEDH, 26 mars 1987, série A nº 116, Leander c/ Suède, § 51.

73 CEDH, 4 mai 2000, req. nº 28341/95, Rotaru c/ Roumanie, §57 ; CEDH, 21 juin 2011 req. nº 30194/09, Shimovolos c/ Russie.