LE PROFILAGE RACIAL À L'ÈRE DE L'INFORMATION

J.M. Porup est un journaliste indépendant s'intéressant à la sécurité nationale et à la cybersécurité basée à Toronto. Ses reportages ont parus dans la SRC, *The Economist*, *Christian Science Monitor*, *Ars Technica*, *Vice Motherboard*, et plusieurs autres. Suivez-le sur Twitter : @toholdaquill.

L'internet déstabilise la démocratie et transforme le Canada en une dictature totalitaire dirigée par une police secrète. Ceci ouvre la voie à des violations des droits de la personne sur une très grande échelle. Des outils informatisés sont créés avec du racisme au cœur de leur système. La prévision policière et les algorithmes de condamnation automatisent le racisme. Le piratage informatique et la surveillance gouvernementale détruisent la démocratie et concentrent le pouvoir dans les mains des terroristes sanctionnées par l'État au Canada — le SCRS, la CST et l'agence secrète de la GRC.

Le profilage racial n'est pas difficile à identifier dans l'espace de la chair (le *meatspace*, qui s'oppose au *cyberspace*). Lorsque la police entreprend de demander à voir les cartes d'identités de certains individus ou lorsqu'elle procède à des fouilles sans avoir de raisons valables de le faire, il est facile de voir le profilage racial à l'œuvre. La prise de conscience d'un problème permet la tenue d'une conversation publique et place des solutions à portée de main.

Mais qu'en est-il de l'internet? Nous avions l'habitude de dire que nous menions nos vies « dans le vrai monde » et nous allions en ligne. Cependant, dans un sens vraiment littéral, nous vivons maintenant en ligne. Même si nous ne touchons jamais à un ordinateur, notre monde est bâti sur des ordinateurs. Et les règles sont différentes dans ce contexte. Le pouvoir dans le cyberespace change la donne et rend possible de nouvelles formes de profilage racial beaucoup moins évidentes.

La Commission ontarienne des droits de la personne (CODP) définit le profilage racial comme :

> ***toute action*** prise pour des ***raisons de sûreté, de sécurité ou de protection du public*** qui repose sur des ***stéréotypes*** fondés sur la race, la couleur, l'ethnie, la religion, le lieu d'origine ou une combinaison de ces facteurs plutôt que sur un soupçon raisonnable, dans le but d'isoler une personne à des fins d'examen ou de traitement particulier. La Commission ajoute que l'âge et le sexe peuvent également avoir une incidence sur l'expérience du profilage racial[1].

1 Rapport d'enquête de la Commission ontarienne des droits de la personne, Un prix trop élevé : Les coûts humains du profilage racial, p. 6. Aussi en ligne : http://www.ohrc.on.ca/fr/un-prix-trop-%C3%A9lev%C3%A9-les-co%C3%BBts-humains-du-profilage-racial/d%C3%A9finition-du-profilage-racial Les mots en gras sont dans l'original.

Dans ce texte, je vais examiner les façons à travers desquelles le profilage racial pourrait ultimement être renforcé par sa reproduction dans le cyberespace à travers les mécanismes suivants : *1)* la prévision policière, *2)* les algorithmes de condamnation, *3)* les outils de piratage ciblé, et *4)* la surveillance de masse.

LA PRÉVISION POLICIÈRE

La prévision policière est une mesure qui vise à prévenir le crime en tentant de prédire où il va se produire à l'avenir. Des algorithmes analysent de grandes quantités de données afin d'identifier les points chauds de la criminalité, ils assignent un « score de dangerosité » aux citoyens qui indique la probabilité qui leur est associée de commettre un crime, et ils aident à déployer les ressources policières plus efficacement[2].

Mais pour que ces algorithmes marchent bien, ils doivent être mis en application de façon impartiale (c'est-à-dire, ces algorithmes doivent être construit de façon impartiale à la base), et ils doivent être utilisés de façon impartiale.

Dans les deux cas, la prévision policière échoue.

Dans les mots que Ronald Bailey a écrits dans *Reason*, « L'exactitude des programmes de prévision policière dépend de l'exactitude de l'information qu'on leur nourrit »[3].

La ACLU de Massachusetts explique « Si nous alimentons un algorithme uniquement avec des données biaisées sur les arrestations, l'algorithme va simplement répéter l'injustice en conseillant aux policiers d'envoyer encore plus d'agents pour patrouiller les quartiers où résident beaucoup de personnes de race noire. Dans ce sens, la prévision policière crée une boucle de rétroaction qui ne fait que renforcer l'injustice »[4].

En d'autres mots, si nos anciennes données sur le maintien de l'ordre nous suggèrent fortement de renforcer la surveillance policière dans certains quartiers pour certains types d'offenses, alors les algorithmes de prévention ne vont faire rien d'autre que de « prédire le passé ».

De plus, ces algorithmes sont créés par des entreprises privées et leurs méthodologies sont cachées du public qu'elles surveillent. Comment ces algorithmes fonctionnent-ils? Ces algorithmes sont-ils intrinsèquement fondés sur des préjugés, qu'ils soient conscients ou inconscients?

Ces méthodes préventives ne devraient-elles pas être accompagnées d'une divulgation complète et ouverte de la façon que le système fonctionne?

Si tout ceci ne suffisait pas pour sérieusement remettre en question la sagesse de la prévention policière, une enquête menée par le *San Francisco Weekly* a conclu qu'il n'y a pas de preuves publiques que la prévention policière est efficace ; « L'avenir du maintien de l'ordre s'apparente beaucoup à une bonne campagne de marketing »[5].

Le *Toronto Star* signale que les méthodes de prévention policière sont déjà mises en place au Canada[6]. Ceci n'augure rien de bon pour l'Ontario et les autres provinces où les données sur les « contrôles policiers de routine » et le fichage (*carding* en anglais) nous révèlent que les Afro-Canadiens et les autres individus racialisés reçoivent déjà une proportion disproportionnée de l'attention policière.

LES ALGORITHMES DE CONDAMNATION

Lorsque les juges assignent des peines dans les tribunaux criminels à travers les États-Unis, dans plusieurs instances, les tribunaux utilisent désormais des algorithmes de condamnation qui assignent une côte à chaque criminelle par rapport à sa probabilité de récidivisme.

Cependant, une enquête menée par ProPublica a découvert que les algorithmes de condamnation comportent des biais défavorables envers les condamnés de race noire[7].

Même l'ancien procureur général américain avait des inquiétudes face aux algorithmes de condamnation. ProPublica signale qu'en 2014 Eric Holder « nous avertissait que les scores de récidivisme ajoutaient certains biais aux tribunaux. Il avait demandé à la Commission américaine sur la détermination de la peine d'en étudier leur usage. " Bien que ces mesures aient été créées avec la meilleure des intentions, je m'inquiète du fait qu'elles sapent involontairement nos efforts d'assurer un système de justice individualisé et impartial " avait-il dit,

2 http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist

3 https://reason.com/archives/2012/07/10/predictive-policing-criminals-crime

4 https://privacysos.org/predictive

5 http://www.sfweekly.com/sanfrancisco/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/Content?oid=2827968

6 https://www.thestar.com/news/gta/2016/05/10/surveillance-and-predictive-policing-welcome-to-the-safety-state-of-tomorrow.html

7 https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

ajoutant, " elles pourrait exacerbées des inégalités injustifiées et injustes qui sont beaucoup trop communes dans notre système de justice criminelle et dans notre société " »[8].

L'enquête de ProPublica avait conclu que :

En tentant de déterminer les individus à risque de récidiver, l'algorithme a commis des erreurs envers les accusés noirs et blancs à peu près au même rythme, mais de façons très différentes.

- La formule était particulièrement susceptible de faussement accuser de récidivisme un individu de race noire, qualifiant à tort de récidiviste un individu de race noire deux fois plus souvent qu'un individu de race blanche.

- Les accusés blancs ont plus fréquemment été qualifiés à tort comme étant à faible risque de récidivisme que les accusés noirs.

L'apprentissage par les machines est de la bureaucratie automatique. Les bureaucrates injectent leurs partis pris et leurs préjugés personnels dans leur travail, souvent de façon inconsciente. Idem pour les programmeurs qui conçoivent et créent ce genre d'algorithmes.

Les prises de décisions qui privent des citoyens de leur liberté ne sont pas améliorées par les préjugés automatiques et puis en nous dissimulant derrière le fonctionnement mystérieux d'un programme informatisé opaque.

Est-ce que les algorithmes de condamnations sont utilisés au Canada? S'ils le sont, est-il même possible de contourner le rôle que le profilage racial joue dans ce type de système?

LES OUTILS DE PIRATAGE CIBLÉ

Les fouilles en l'absence de soupçons menées par la police qui sont basées sur la race, la religion, ou le pays d'origine violent le Code des droits de la personne de l'Ontario — autant en ligne que dans la réalité.

Les départements de police du monde entier accèdent systématiquement aux téléphones intelligents, portables, tablettes, même aux appareils domestiques connectés à l'internet, par exemple à l'Amazon Echo, dans le but d'écouter les conversations des accusés en utilisant les microphones de leurs appareils ou afin de les épier en usant les caméras intégrées aux appareils[9]. En juin 2016, une cour d'appel américaine a statué que la police n'avait pas besoin d'un mandat pour accéder aux appareils d'un suspect[10].

Le piratage en l'absence de soupçons, qui s'apparente à une fouille ciblée de nos téléphones et autres appareils intelligents, est en train de devenir une norme dans le monde entier. De telles fouilles touchent démesurément les groupes racialisés étant donné que, dans notre ère nouvelle, la sécurité des téléphones intelligents est devenue un produit de luxe moins accessible aux plus pauvres, les rendant plus vulnérables aux abus criminels et policiers. Par exemple, alors que le iPhone de Apple est reconnu comme étant un des téléphones les plus sécuritaires, contrairement au système d'exploitation de Google Android, qui lui, bien que généralement plus abordable, est vivement critiqué pour sa faible sécurité. Ceci met les usagers à risque non seulement par rapport aux programmes malveillants qui sont motivés financièrement, mais permet aux forces de l'ordre de facilement se pirater un accès jusque dans leurs téléphones. Les mesures sécuritaires insuffisantes d'Android laissent la porte ouverte au profilage racial par la police qui s'engage dans du piratage de cellulaires en l'absence de raisons valables.

Dans le cas où cette pratique n'est pas encore courante, il semblerait que les forces policières canadiennes soient très intéressées par l'acquisition d'outils de piratage. Quelles sont les règles qui gouvernent ultimement leurs utilisations par les forces policières, notamment par les Services de police de Toronto[11]? Qu'est-ce qui empêche les services de police dans toutes les provinces de faire usage de techniques de piratage pour avoir accès aux appareils connectés à l'internet sur des soupçons de nature raciale?

LA SURVEILLANCE DE MASSE

En 2013, les fuites de renseignements de la National Security Agency (NSA) des États-Unis par Edward Snowden, le dénonciateur et ancien employé de la Central Intelligence Agency, ont révélé que la surveillance de masse est une pratique répandue et proéminente des services de surveillance non seulement américains, mais également canadiens. Plus précisément, des messages privés entre virtuellement tous les

8 *Ibid.*

9 https://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech

10 https://www.eff.org/deeplinks/2016/06/federal-court-fourth-amendment-does-not-protect-your-home-computer

11 https://news.vice.com/article/canadian-police-spies-eyed-hacking-team-tech-and-the-law-now-makes-it-easier-to-acquire

citoyens sont recueillis, stockés et analysés sans que ceux-ci en soient conscients et sans leur consentement.

La NSA stocke ces données avec les messages recueillis par les autres membres de l'alliance d'espionnage Five Eyes (FVEEYES), qui comprend les agences d'espionnage des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande.

Analyser le grand nombre de données recueillies nécessite que ces agences d'espionnage fassent usage d'algorithmes afin d'automatiser ce processus. Comme je l'ai mentionné plus tôt, la NSA utilise un algorithme d'apprentissage automatique afin d'assigner un score à chaque citoyen par rapport à sa probabilité de prendre part à une activité terroriste[12]. Le trafic téléphonique d'une nation complète a été analysé afin de coter les citoyens par rapport à leur 'potentiel terroriste'. L'algorithme SKYNET de la NSA s'est avéré imparfait et a identifié à tort des milliers de Pakistanais comme terroristes, qui peut-être ont par la suite été surveillés avec acharnement par drone.

Bien que de telles révélations n'aient pas encore été divulguées par rapport à aucune agence canadienne, il est fort possible qu'un algorithme d'apprentissage automatisé similaire soit utilisé pour coter les citoyens et les résidents canadiens par rapport à leur probabilité de prendre part à une activité terroriste ou criminelle. Ceci faciliterait certainement la validation des types de profilage racial qui sont déjà beaucoup trop répandus dans notre société.

CONCLUSION

La lutte pour la défense des droits de la personne se trouve désormais dans le monde virtuel. De plusieurs façons, les technologies de l'information rendent possibles les violations des droits de la personne à l'échelle mondiale. Les outils de piratage et de surveillance de masse utilisés par les agences d'espionnage et les services policiers compromettre l'État de droit et viole les droits de la personne. L'utilisation de la prévision policière et des algorithmes de condamnation est de plus en plus considérée comme acceptable, malgré les exemples clairs du rôle que le profilage racial joue dans leurs fonctions.

La défense des droits de la personne, telle que concrétisée dans le Code, nécessite que nous examinions les abus qui sont faits non seulement « dans le vrai monde », mais également dans le monde virtuel.

12 http://arstechnica.co.uk/security/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people