Criminologie

La criminologie de l'information : état des lieux et perspectives

Francis Fortin et Olivier Delémont

Volume 52, numéro 2, automne 2019

La criminologie de l'information : état des lieux et perspectives

URI : https://id.erudit.org/iderudit/1065853ar
DOI : https://doi.org/10.7202/1065853ar

Aller au sommaire du numéro

Éditeur(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (imprimé)
1492-1367 (numérique)

Découvrir la revue

Citer ce document

Fortin, F. & Delémont, O. (2019). La criminologie de l'information : état des lieux et perspectives. *Criminologie*, *52*(2), 5–12. https://doi.org/10.7202/1065853ar

La criminologie de l'information : état des lieux et perspectives

Francis Fortin
Professeur agrégé
École de criminologie, Université de Montréal
francis.fortin@umontreal.ca

Olivier Delémont
Professeur ordinaire
École des sciences criminelles, Université de Lausanne
olivier.delemont@unil.ch

Pour beaucoup, l'entrée dans le troisième millénaire marque l'avènement d'un tournant majeur dans l'histoire de l'humanité. Après les développements de l'agriculture et de l'élevage, qui ont favorisé la sédentarisation des populations, l'invention de l'imprimerie, qui a permis la diffusion des connaissances et catalysé les développements scientifiques, et la révolution industrielle, caractérisée par ses transformations économiques, sociales et politiques, la révolution numérique amorcée dès les années 1950 et dont nous sommes tous les témoins privilégiés est en train de bouleverser de manière profonde et certainement durable l'organisation et les échanges entre les sociétés. L'ère numérique redéfinit le partage des connaissances et les communications entre les individus. Au-delà des évolutions technologiques, elle induit d'importantes transformations sociétales qui redéfinissent les mécanismes et échanges entre les acteurs des sociétés contemporaines. Certaines pratiques changent, évoluent, voire disparaissent, alors que de nouvelles formes d'interactions, d'espaces ou de temporalités apparaissent. Cette mutation n'épargne bien évidemment pas les sciences concernées par l'étude du crime, la criminologie en tête. L'ère numérique s'accompagne non seulement d'une redéfinition des contours de l'objet de la crimino-

logie, mais aussi d'une évolution dans sa manière de l'exercer, que ce soit sur le plan des questions qu'elle étudie ou des méthodes sur lesquelles elle peut s'appuyer.

Alors que nous expérimentons au quotidien les effets de ce tournant numérique de l'humanité, il nous est apparu important de consacrer la thématique d'un numéro spécial de la revue *Criminologie* aux enjeux et perspectives qui accompagnent les technologies de l'information et du numérique. Depuis plusieurs décennies, la criminologie étudie l'impact de l'informatisation sur la société, explorant en particulier les conséquences de l'arrivée d'Internet et de la mise en réseau des ordinateurs sur le crime et le criminel. Mais dans le cadre de ce numéro thématique, nous avons tenté d'étendre le champ d'études, en considérant plusieurs dimensions complémentaires. Il nous importe bien entendu de refléter les transformations que la numérisation impose sur l'objet d'étude, que ce soit par la modification de certains comportements (articles de Bergeron, Delle Donne et Fortin, et de Guillot et Décary-Hétu) ou l'apparition de nouveaux comportements (article de Estano). Nous voulons aussi souligner les évolutions induites en termes d'outils de recherche, en mettant en exergue la consolidation de nouveaux moyens de mesure fondés sur l'exploitation des données disponibles dans les sources ouvertes (articles de Caneppele et collègues et de Da Silva, Boivin et Fortin), ou le rôle du traitement informatisé des données pour la compréhension de certaines formes de criminalité (article de Chopin et Aebi). La démarche de collecte et d'organisation systématique de données numériques est souvent mise en balance avec un impératif de maintien de la confidentialité et de protection de la sphère privée des individus ; c'est pourquoi il nous paraît utile d'aborder cette question sous l'angle d'un exemple pratique relatif au délai de conservation de profils génétiques de personnes dans une banque de données (article de Cinaglia et collègues). Et enfin, il nous semble pertinent d'étudier comment la compréhension du rôle des intervenants de terrain, en l'occurrence en matière d'investigation de scène d'infraction, est perçue en cette ère de transformation numérique (article de Mousseau).

Ainsi, l'objectif de ce numéro est de mettre en lumière ces nouveaux enjeux dans un contexte d'utilisation problématique, de non-conformité ou d'actes criminels. Puisque ces enjeux touchent les individus, les gouvernements et les entreprises à différents degrés, ce numéro suscitera un vif intérêt tant dans les communautés de pratiques que pour les chercheurs en criminologie et la population en général.

Nouvelles formes de criminalité et nouvelles façons de l'observer

Une des façons de présenter comment les « nouveaux » environnements virtuels peuvent stimuler de nouvelles formes d'activités criminelles consiste à voir comment le crime interagit avec la machine (Wall, 2007). Dans cette perspective, les transformations des activités criminelles induites par l'arrivée des technologies de l'information peuvent se décliner en trois types : les crimes *contre* la machine, les crimes *qui utilisent* la machine et les crimes *dans* la machine (Wall, 2007). Cette dernière forme d'actions peut, par exemple, s'illustrer dans les activités du groupe Wikileaks qui exploite la production participative rendue possible par Internet pour parvenir à ses fins. Les espaces virtuels permettent d'échanger l'information nécessaire à la commission d'infraction et deviennent donc des sujets d'étude essentiels pour les responsables des actions de sécurité (voir Cusson, 2008).

L'évolution des habitudes de vie inhérentes à la digitalisation de nos sociétés permet aussi l'émergence de nouveaux comportements qui échappent aussi à certaines formes de classification. C'est notamment le cas du *swatting*, stratégie de harcèlement d'un individu qui consiste à déclencher l'intervention d'une unité spéciale d'élite de la police par la fausse annonce d'une situation d'urgence (alerte à la bombe, prise d'otages, acte suicidaire, etc.). Alors que plusieurs exemples avec des conséquences parfois funestes ont été rapportés en Amérique du Nord, ce type de comportement a plus récemment fait son apparition en France. Dans son article, Estano essaye de décrypter ce phénomène, ses motivations et ses possibles conséquences, en adoptant une approche clinique fondée sur l'étude de cas concrets.

Pour les agences d'application de la loi, les données disponibles en sources ouvertes ont jadis été considérées comme des ressources de dernier recours. L'apparition des nouveaux environnements et la généralisation des systèmes d'information ont toutefois changé la donne : les renseignements en source ouverte sont devenus des outils essentiels, pierre angulaire pour la compréhension de plusieurs formes de comportements criminels. L'observation des groupes extrémistes et d'activités par le biais des informations publiquement disponibles est désormais devenue un incontournable. Les individus et les groupes qui représentent des menaces du fait de leur idéologie extrémiste, ou par la violence qu'ils appellent de leurs vœux, ont besoin des nouveaux médias pour diffuser leur idéologie, leurs croyances, leurs objectifs et tenter de

persuader d'autres personnes d'adhérer au mouvement (Carter, 2004). Or, le suivi et l'analyse des activités de ces individus ou groupes par les chercheurs ou les gestionnaires de sécurité publique reposent largement sur des données et des outils (les médias sociaux, notamment) qui sont les mêmes que ceux qu'emploient les adeptes des idéologies pour leurs démarches de recrutement. L'avantage d'avoir accès à ces données devient dès lors évident, puisqu'elles véhiculent une connaissance directe des actions que le groupe commande à ses membres, de la mesure du taux d'acceptation ou de popularité du groupe ou de l'idéologie. Le « J'aime », le partage et les commentaires deviennent ainsi un indicateur utile, bien qu'imparfait, de la popularité des messages et des revendications de ces individus ou groupes.

Parmi ces groupes d'activistes ayant mobilisé les nouveaux espaces virtuels, on peut évoquer Anonymous, un groupe d'individus reconnu pour s'impliquer dans des mouvements sociaux visant à défendre différentes causes (Coleman, 2014 ; Milan, 2013 ; McGovern et Fortin, 2019). Par le passé, certains membres ont utilisé des moyens illégaux afin de manifester leurs idées (Coleman, 2014 ; Klein, 2015). Dans la perspective de l'article de Bergeron, Delle Donne et Fortin, les activités de ce groupe Anonymous sont examinées au travers des publications de la communauté Facebook des groupes s'identifiant à Anonymous au Canada. Bien que des similarités et des différences entre les sous-groupes régionaux soient mises en exergue, cette étude empirique révèle que le risque que représente le groupe Anonymous en termes de commission de gestes de violence ou autres activités illégales est restreint. Les résultats montrent que les comptes des réseaux sociaux s'identifiant à Anonymous sont davantage portés sur le travail de réputation du groupe aux yeux de la population que sur l'organisation d'actions concrètes. Ceci suggère que l'activisme (ou *hacktivism*) en temps de paix ne fait que chuchoter en attente d'un plus grand désordre comme ce fut le cas lors des manifestations du Printemps érable au Québec où le collectif Anonymous avait divulgué les renseignements personnels de membres de l'Association des directeurs de police du Québec en guise de représailles aux actions policières.

Les espaces virtuels permettent aussi le développement d'une criminalité de marché où clients et vendeurs exploitent ces nouveaux espaces comme interfaces pour la vente de produits illicites. Dans leur article, Guillot et Décary-Hétu observent que les cryptomarchés constituent des zones de convergence efficientes pour la vente d'infor-

mations permettant d'éventuelles fraudes de carte de crédit (*carding*). En plus de faciliter la rencontre entre ces acteurs mis en confiance par la forme d'anonymat qu'elles offrent, les plateformes en ligne permettent l'échange de l'ensemble des produits et services nécessaires à la commission de ce crime. De plus, il est observé que la sophistication du mécanisme d'évaluation implanté sur ce type de plateforme contribue à en accroître la confiance et assure la pérennité des activités des trafiquants.

Da Silva, Boivin et Fortin s'appuient sur une analyse du contenu des médias sociaux pour prédire la criminalité urbaine. Ils exploitent les données circulant dans ses environnements virtuels pour tenter de découvrir ce qui se passe dans les espaces physiques de la vie réelle. Considérant les médias sociaux comme le reflet des comportements humains, ils en étudient la valeur en tant qu'indicateur pour apprécier la distribution de comportements illicites.

Le potentiel informatif qu'offre le traitement de données issues de sources ouvertes à des fins d'analyse criminologique est également au cœur de l'étude exploratoire proposée par Caneppele, Cinaglia, Sperrer et Langlois. Par la collecte, l'intégration et l'analyse du contenu d'articles de presse librement disponibles relatant des violations à l'intégrité sportive, les auteurs de cette étude montrent comment cette démarche peut permettre de tracer le portrait de la répartition géographique de ces menaces à l'intégrité sportive.

Les nouveaux enjeux du numérique en matière d'utilisation et de conservation des données

Dans la foulée de l'informatisation de la société, on a pu observer une migration progressive des données personnelles vers des systèmes d'information de plus en plus complexes et centralisés. Selon les acteurs impliqués, ces informations peuvent prendre plusieurs appellations : renseignements criminels, renseignements personnels ou données personnelles. L'existence sur des plateformes numériques de telles informations caractérisant les individus ou leurs comportements induit des préoccupations et des responsabilités pour toutes les instances de la société. La collecte, la conservation, l'analyse et la diffusion de ces informations deviennent des enjeux majeurs dans la définition et la pérennisation des sociétés démocratiques. Mais en parallèle, comme les données constituent des denrées très précieuses – le nouvel or noir –,

d'importants efforts sont déployés pour exploiter ces données et en retirer une utilité.

Ces informations sensibles vont au-delà des informations nominatives traditionnelles. On y retrouve maintenant des données de géolocalisation, des informations sur les centres d'intérêt et les passe-temps, sur les sites web visités, les relations amicales, le contenu de conversations sur les médias sociaux, etc. Jusqu'à tout récemment, la conservation et l'utilisation de telles données sensibles demeuraient l'apanage des gouvernements, et le spectre de Big Brother représentait la principale menace associée à l'exploitation abusive (par l'État) de ces informations personnelles. Mais le récent scandale de Cambridge Analytica, combiné avec les répétitives révélations de diverses brèches de sécurité, a dévoilé un tout autre pan d'exploitation douteuse mettant en péril la notion même de sphère privée, et susceptible d'avoir des conséquences importantes. Le monde a pris conscience qu'en plus des pouvoirs publics, les entreprises privées, et en particulier les géants du numérique comme Google, Amazon, Facebook, Apple ou Microsoft, accumulaient, utilisaient et revendaient des informations personnelles sur les utilisateurs.

De nombreux rapports ont permis de dégager les préoccupations reliées à l'utilisation et à la conservation des données personnelles des citoyens. Il n'y a pas si longtemps, au Québec, des craintes par rapport à l'utilisation de données personnelles avaient déjà été formulées en lien avec les enjeux éthiques associés à l'utilisation des caméras de surveillance dans les lieux publics et l'utilisation de données biométriques. Ces discussions avaient débouché sur la rédaction par un groupe d'experts d'un rapport qui proposait d'instaurer un juste équilibre entre les libertés fondamentales et le besoin de sécurité, entre la liberté et la répression (voir Commission de l'éthique de la science et de la technologie, 2008). En une décennie, les technologies se sont développées, mais les préoccupations demeurent les mêmes. Et récemment, on a vu des débats similaires foisonner autour de la recherche d'un équilibre entre les technologies de surveillance des téléphones mobiles et les préoccupations de préservation de la sphère privée (Bennett, Haggerty, Lyon et Steeves, 2014).

L'État, dans l'exercice de ses fonctions régaliennes, collecte également des données qui portent atteinte à la sphère privée. Il devient alors le gardien de l'intégrité et de l'utilisation de cette information. En ce sens, un certain nombre d'exigences et de devoirs lui sont imputables, afin d'éviter notamment des dérives d'utilisation abusive communément

désignées sous le terme de *function creep* (Dahl et Sætnan, 2009). En matière de lutte contre la criminalité, la question de la constitution, de la gestion et de l'utilisation de banques de données ADN a été, et continue d'être, un sujet largement débattu. En particulier, la problématique de la durée de conservation des profils génétiques de personnes condamnées par la justice fait l'objet de discussions nourries, puisqu'elle met à l'épreuve des notions apparemment antinomiques que sont le droit à l'oubli et la sécurité de l'État. Mais les différentes prises de position reposent davantage sur des croyances que sur des données quantitatives, bien maigres en la matière. C'est précisément pour combler un peu cette carence que Cinaglia, Chopin, Villetaz et Delémont, ont traité les données issues de la banque de données ADN suisse pour mesurer l'impact concret de différents délais putatifs d'effacement de profils ADN. Les résultats de cette étude ont d'ailleurs été pris en considération dans le cadre des travaux législatifs portant sur la révision de la loi sur l'ADN.

Un autre enjeu important de l'exploitation des données que nous offrent les outils actuels du numérique est celui de leur utilisation. Face à cette effervescence de données, il devient éminemment difficile de ne pas être submergé et de pouvoir en retirer une information fiable et intéressante. Ce défi, qui s'apparente à quelques égards à la recherche de l'aiguille dans la botte de foin, est complexe ; et bien souvent, on considère que le salut viendra des mathématiques, de la statistique et de l'informatique, rassemblées sous le label de *data science*, mais la recherche réalisée par Chopin et Aebi nous rappelle que le criminologue a un rôle primordial à jouer. En redéfinissant le rôle du scientifique dans le paysage judiciaire, Chopin et Aebi montrent qu'une analyse des données colligées dans le système de gestion des liens de cas d'agressions sexuelles en France permet d'envisager une meilleure application de cet outil dont l'utilité actuelle est largement remise en question.

La transformation numérique de notre société force de nombreuses professions à repenser leurs rôles et les contours de leurs pratiques. Et tout ce que nous avons dit jusqu'à présent nous conforte dans l'idée qu'il doit en aller de même pour les sciences criminelles. Comment ne pas être convaincu que le criminologue va devoir progressivement repenser sa place dans les mutations que le numérique induit sur le crime ? Et de son côté, comment est-ce que les acteurs de la police scientifique perçoivent les changements qui impactent leur discipline ? C'est dans cette optique que peut se lire l'étude menée par Mousseau,

qui dévoile la perception du rôle du technicien de scène de crime par les gestionnaires de police. Cette étude montre que la contribution de ces premiers maillons de la chaîne criminalistique est perçue davantage dans une perspective technique que comme une activité scientifique. Une vision qui paraît un peu surannée au regard des profonds bouleversements que subit notre société.

Les articles réunis dans ce numéro spécial ne sont qu'un aperçu de ce qui deviendra vraisemblablement un axe de recherche prolifique au cours des prochaines années. Ainsi, la dématérialisation des infractions au sein des espaces virtuels est déjà bien amorcée alors que les préoccupations en lien avec l'utilisation et la conservation des informations par les organismes se sont déjà bien manifestées. On peut déjà entrevoir que ces questions continueront d'alimenter les études au sein d'un nouvel axe de recherche, le présent numéro ne constituant qu'un échantillon.

Références

Bennett, C. J., Haggerty, K. D., Lyon, D. et Steeves, V. (dir.). (2014). *Vivre à nu : la surveillance au Canada*. Athabasca, Alberta : Athabasca University Press.

Carter, D. L. (2004). *Law enforcement intelligence : A guide for state, local, and tribal law enforcement agencies*. Washington, DC : U.S. Department of Justice, Office of Community Oriented Policing Services.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy : The many faces of anonymous*. Londres, Royaume-Uni : Verso.

Commission de l'éthique de la science et de la technologie. (2008). *Viser un juste équilibre. Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*. Québec, Québec : Gouvernement du Québec.

Cusson, M. (2008). De l'action de sécurité. Dans M. Cusson, B. Dupont et F. Lemieux (dir.), *Traité de sécurité intérieure* (p. 43-57). Lausanne, Suisse : Presses Polytechniques et Universitaires Romandes (PPUR).

Dahl, J. Y. et Sætnan, A. R. (2009). "It all happened so slowly" – On controlling function creep in forensic DNA databases. *International Journal of Law, Crime and Justice*, *37*(3), 83-103.

Klein, A. G. (2015). Vigilante media : Unveiling Anonymous and the hacktivist persona in the global press. *Communication Monographs*, *82*(3), 379-401.

McGovern, V. et Fortin, F. (2019). The Anonymous collective : Operations and gender differences. *Women & Criminal Justice*, 1-15. https://doi.org/10.1080/08974454.2019.1582454

Milan, S. (2013). WikiLeaks, Anonymous, and the exercise of individuality : protesting in the cloud. Dans B. Brevini, A. Hintz et P. McCurdy (dir.), *Beyond WikiLeaks* (p. 191-208). Londres, Royaume-Uni : Palgrave Macmillan.

Wall, D. S. (2007). *Cybercrime : The transformation of crime in the information age*. Cambridge, Royaume-Uni : Polity.