CRI 6720 : IMPACT DES TECHNOLOGIES DE SÉCURITÉ

Plan de cours – Hiver 2021

Ma. 13h00-15h00 – Zoom

Samuel Tanner – professeur agrégé
École de criminologie – Université de Montréal
Bureau C-4100

t : (514) 343-6111 # 40567
e : samuel.tanner@umontreal.ca

Disponibilités : sur rendez-vous par courriel

1. Introduction

Les dernières décennies ont connu des transformations majeures de la gouvernance en matière sociale, politique, économique et de sécurité. En particulier, la substitution d'une philosophie du *New Public Management,* issue du néo-libéralisme, à un modèle dit providentiel, ou d'État social, a non seulement provoqué une cure d'amaigrissement des institutions publiques, y compris en matière de sécurité, mais a aussi imposé à ces organismes une rhétorique d'efficience, d'imputabilité et d'obligation de résultat, autant de critères issus de la sphère privée. Contraints par ces impératifs d'une part, mais aussi par des ressources de plus en plus limitées d'autre part, les acteurs de la sécurité, dont la police en première ligne, ont connu des bouleversements et transformations majeurs de leur fonctionnement et de leurs politiques. Optant pour des modèles de gouvernance de la sécurité offrant une redistribution de responsabilités (ex. police communautaire), c'est aussi par l'adoption toujours plus grande de technologies de sécurité qu'ils ont tenté de répondre aux nouveaux impératifs de leur mission. Les technologies de sécurité ne sont pourtant pas récentes et l'histoire montre que leur existence est concomitante à celle des métiers de la sécurité. Or, depuis les bouleversements provoqués par la philosophie du *New Public Management*, elles occupent une pondération toute particulière dans le discours, les politiques et les pratiques de sécurité. L'avènement du Big Data, de l'intelligence artificielle et de la rationalité algorithmique, la banalisation des caméras de surveillance portées par les policiers, ou présentes dans les rues ou la biométrie et les scanners corporels dans les aéroports sont autant de nouvelles technologies, ou de « machines », qu'il est nécessaire d'appréhender à travers les débats politiques, scientifiques stratégiques et pratiques qui les accompagnent. Au-delà d'une perspective dite de la « boîte noire », qui envisage ces nouvelles technologies d'un point de vue fonctionnaliste et déterministe, ou par leurs effets, elles nécessitent, tout comme leur évolution, d'être considérées dans leur insertion sociale, politique, idéologique, mais aussi de leurs

conséquences en matière de justice sociale et de discrimination. Au même titre que leur espace de formulation, l'utilisation et l'appropriation des nouvelles technologies doivent s'appréhender dans le contexte social, politique, économique et idéologique de leurs utilisateurs. Enfin, et en dépit de l'accent marqué pour les effets des « nouvelles » technologies, il ne faut pas pour autant oublier la présence du « low-tech », tel le fichier papier ou le barbelé, et leur articulation avec les nouvelles technologies dans l'accomplissement des missions de sécurité, qu'il s'agisse du secteur public ou privé.

2. Objectif général du cours

Le cours vise à sensibiliser et stimuler la réflexion des étudiants quant aux principaux enjeux qui caractérisent la formulation, le déploiement, l'appropriation et l'impact d'une technologie de sécurité, tant d'un point de vue social qu'individuel. Comme l'indique l'intitulé du cours, il s'agira de fournir un cadre qui permettra d'appréhender et comprendre l'impact des technologies de sécurité et développer une réflexion critique et intégratrice des dimensions historique, politique, sociale et performative (effets) – et parfois inattendus – des technologies de sécurité. Pour ce faire, nous procéderons en quatre blocs thématiques. Dans un premier temps, nous nous intéresserons aux débats caractérisant l'appréhension même de la technologie dans sa genèse, sa politique et sa conceptualisation. Un second bloc portera, quant à lui, sur la formulation d'une technologie, ainsi que son appropriation pratique. Nous nous intéresserons ensuite aux rapports entre surveillance et technologie à l'ère « post-révélations » Snowden, avec un intérêt particulier pour le tournant « Big Data » en matière de surveillance. Enfin, un dernier bloc traitera de deux formes particulières de technologie contemporaines, soit l'impact des technologies numériques en matière de participation sociale et de radicalisation, l'impact des algorithmes en matière de gouvernance de la sécurité et se terminera par une réflexion éthique sur la relation entre technologie et race, discrimination.

3. Pédagogie et enseignement

En raison du contexte sanitaire actuel et de pandémie de COVID-19, l'ensemble du séminaire **se déroulera à distance**, sur la plateforme Zoom. Selon le principe qui caractérise la formation étudiante aux 2e et 3e cycles, le bon déroulement du séminaire repose largement sur la responsabilité des étudiant(e)s **dont la présence et la participation sont nécessaires**. Dans cet esprit, les étudiants sont invités à garder leur caméra allumée. Les séances sont principalement alimentées par les interventions et réflexions des étudiant(e)s, aussi **ils/elles ont la responsabilité de lire les textes prévus pour chacune des séances**, indiqués ci-dessous, et disponibles sur la plateforme StudiUM. Il est donc crucial de lire les textes puisqu'une grande partie des séances sera alimentée par les réflexions, commentaires, questions des étudiant.e.s. le professeur, quant à lui, apportera des éléments théoriques, conceptuels et méthodologiques nécessaires au déroulement des discussions.

Un duo d'étudiant.e.s sera désigné.e pour chaque séance[1] et qui aura la responsabilité d'animer la séance à partir des lectures identifiées. Chaque duo se composera d'une personne qui réalise un rapport intégratif des lectures pour la séance (précisions ci-dessous) et d'une personne qui

[1] Pour des raisons logistiques, il se peut qu'il y ait plus qu'un duo pour certaines séances.

réalise une critique du rapport du / de la collègue, sur le mode de la complémentarité. Fonctionnant par équipe, le duo aura pour responsabilité d'animer la séance, de poser des questions à l'ensemble des participants du séminaire et d'animer la discussion autour des textes, avec l'aide du professeur (ex. par des illustrations ou des cas d'actualité, à partir d'expériences personnelles ou d'enjeux sociaux et politiques, etc.). Cette organisation vise à promouvoir des séances animées et interactives et des apprentissages dynamiques.

4. Évaluation

L'évaluation se fera **en quatre temps**.

1. Premièrement, les étudiant(e)s seront évalué(e)s sur leur **participation** (prise de parole, participation aux débats, commentaires sur les lectures, animation du séminaire) (10%).
2. **Deuxièmement,** chaque étudiant(e) devra réaliser **un rapport intégratif et critique des lectures** indiquées pour une séance (max. 5 pages), basé sur une grille indicative présentée lors e la première séance du cours et disponible sur StudiUM (20%). Ce rapport, en **format Word**, devra être envoyé par courriel au professeur **au plus tard le samedi midi (12h) précédent le cours**. Il sera aussitôt rendu disponible sur le StudiUM.
3. **Une troisième évaluation** consiste à rédiger **un commentaire / critique d'un rapport du / de la collègue** (max. 3 pages) (20%) et qui suivra la présentation de son rapport. La personne qui rédige le rapport écrit, ainsi que la personne rédigeant le commentaire, formeront le duo responsable d'animer la séance. Cette critique sera remise au professeur au plus tard au début de la séance (format Word).
4. Enfin, une **quatrième évaluation** consiste à livrer **un travail de fin de session – 20 pages maximum, interligne 1,5 – traitant d'un sujet libre de choix pour autant qu'il soit en lien avec à l'impact des technologies en sécurité**. À titre d'exemple, ce travail peut traiter d'une technologie, d'un acteur, d'une politique, d'un marché, etc. Ce travail comptera pour 50% de l'évaluation du cours et devra être remis en version électronique (Word) **le 20 avril à 17h00**.

Selon la politique de l'École de criminologie, les travaux remis en retard seront pénalisés de 10% le premier jour et 5% par jour supplémentaire de retard (incluant samedi et dimanche ainsi que les jours fériés). Seules des raisons médicales accompagnées d'un billet du médecin feront exception à cette règle. Ce délai ne peut dépasser 5 jours.

5. Calendrier des rencontres

Séance 1 | 19 janvier 2021 – Introduction, présentation du cours

Présentations des participants et du plan de cours ; organisation de la session (choix des textes par les étudiant.e.s pour leur rapport/commentaire) ; présentation de la grille de rédaction de rapport / commentaire ; introduction à la question de l'impact des technologies en sécurité intérieure.

Bloc 1 | Penser la technologie.

Séance 2 | 26 janvier 2021 – Déterminisme ou neutralité de la technologie ?
Quel statut donner à la technologie : la thèse du déterminisme technologique et le principe de neutralité technologique ; questionnement sur l'autonomie et la performativité des technologies de sécurité.

Lectures :

- Latour, B. (2007), « Le dédale de la médiation technique », in *L'espoir de Pandore. Pour une vision réaliste de l'activité scientifique*, Paris : La Découverte, pp. 183-227.
- Bourne, M. (2012). « Guns don't kill people, cyborgs do : a Latourian provocation for Transformatory arms control and disarmament ». *Global Change, Peace and Security*, 24(1) : 141-163.

Séance 3 | 2 février 2021 – (Dis)continuité dans l'histoire des technologies de sécurité
Retour sur l'histoire contemporaine des technologies de surveillance ; du papier à la biométrie : réflexion sur les technologies d'identification à des fins de sécurité.

Lectures :

- Ceyhan, A. (2006). « Enjeux d'identification et de surveillance à l'heure de la biométrie ». *Cultures & Conflits*, 64 : 33-47.
- Scheel, S. (2019), "Biometric rebordering revisited", in Scheel, S. (2019), *Autonomy of Migration? Appropriating Mobility with Biometric Border Regimes*. Londres: Routledge, pp. 18-41.

Séance 4 | 9 février 2021 – Évolution linéaire ou reconfiguration permanente de la technologie ?
Le barbelé et les murs de sécurité : « succès » persistant d'anciennes technologies dans les dispositifs de sécurité actuels ; les mécanismes d'articulation entre anciennes et nouvelles technologies ; technologies et style de raisonnement.

Lectures :

- Bonelli, L. & Ragazzi, F. (2014). « Low-tech security: Files, notes and memos as technologies of anticipation ». *Security Dialogue*, 45: 476-493.
- Huey, L. & Nahan, J. (2012). « 'We don't have these laser beams and stuff like that': police investigations as low-tech work in a high-tech world », in S. Leman-Langlois, Technocrime : Policing and Surveillance. New York : Routledge : 79-90.

Séance 5 | 16 février 2021 – Théorie et concepts
La technologie comme défi intellectuel ; penser la technologie au-delà de son impact et de ses conséquences ; théorie de l'acteur-réseaux ; les objets techniques, leur conception et leurs utilisateurs.

Lectures :

- Akrich, M. (2006), « Les objets techniques et leurs utilisateurs : de la conception à l'action », in Akrich, M. ; M. Callon & B. Latour (dirs), *Sociologie de la traduction : textes fondateurs*. Paris : Les Mines, pp. 179-199.
- Callon, M. (2006), « Sociologie de l'acteur réseau », in Akrich, M. ; M. Callon & B. Latour (dirs), *Sociologie de la traduction : textes fondateurs*. Paris : Les Mines, pp. 267-276.

Bloc 2 | Politique de la technologie et technologie en pratique

Séance 6 | 23 février 2021 – Espace de formulation et de conception de technologies de sécurité
Entre critères techniques et arbitrages politiques, le processus de choix et de sélection d'une technologie de sécurité ; une constellation d'intérêts et de conflits de rationalité : le processus de fabrication et d'installation d'une technologie de sécurité ; la technologie comme instrument de l'action publique.

Lectures :

- Bellanova, R. & González Fuster, G. (2013). « Politics of disappearance : scanners and (unobserved) bodies as mediators of security practices ». *International Political Sociology*, 7(2), pp. 188-209.
- Newlands, Gemma et al. (2020), "Innovation Under Pressure: Implications for Data Privacy During the Covid-19 Pandemic", *Big Data & Society*, July-December: 1-14.

Séance 7 | 9 mars 2021 – Mobilisation, appropriation et résistance aux technologies : les caméras portatives et la police.
Réflexion sur les 'manières de faire' et les opérations des usagers de technologie de sécurité ; penser la 'consommation' ou l'usage d'une technologie comme une forme de production ; l'importance du contexte d'action et de mobilisation d'une technologie ; le cas des caméras portables et la police.

Lectures :

- Tanner, S. & M. Meyer (2015). « Police work and new security devices: a tale from the beat ». *Security Dialogue*, 46(4): 384-400.
- Marthinus, C., K.; J. J. Willis & S. D. Mastrofski (2019), « The effects of body-worn cameras on police organization and practice es: a theory-based analysis », *Policing and Society*, 29(8), pp. 968-984.

Bloc 3 | Technologie et surveillance

Séance 8 | 16 mars 2021 – La surveillance et la question du *Big Data*
Surveillance et assemblages technologiques ; 'datafication' et traçabilité de la vie quotidienne ; gouvernance algorithmique, intelligence artificielle et enjeux autour du Big data ; rapports humains-machines.

Lectures :

- Aradau, C. & T. Blanke (2015), « The (Big) Data-security assemblage: Knoweldge and critique ». *Big Data & Society*, July-December, 1-12.
- Heath-Kelly, C. (2017), « Algorithmic autoimmunity in the NHS: Radicalisation and the clinic», *Security Dialogue*, 48(1), 29-45.

Séance 9 | 23 mars 2021 – technologies de prédiction et police

Impact du *big data* et de l'intelligence artificielle sur les modèles policiers et de sécurité de lutte contre le crime ; application de la loi guidée par les données ; technologies de prédiction de la délinquance ; enjeux éthiques et légaux.

Lectures :

- Vayre, J.S. (2018), « Comment décrire les technologies d'apprentissage artificiel ?», *Réseaux*, 211(5), pp. 69-104.
- Benbouzid, B. (2018), « Quand prédire c'est gérer. La police prédictive aux États-Unis », *Réseaux*, 211(5), pp. 221-256.

Bloc 4 | Formes de technologies

Séance 10 | 30 mars 2021 – Technologies de l'information (h)activisme et radicalisation

Participation sociale et outils numériques ; le web comme 'espace d'incubation' ; radicalisation et et extrémisme violent en ligne ; usages des technologies de l'information dans la mobilisation des idées et des personnes ; stratégies de lutte contre l'extrémisme violent.

Lectures :

- Tanner, Samuel ; Valentine Crosset & Aurélie Campana (2020), « Far-Right Digital Activism as Technical Mediation : Anti-Immigration Activism on YouTube », in Trottier, Daniel et, al. *Introducing Vigilante Audiences*. Cambridge : Open Book Publisher : pp. 129-160.
- Huey, L. (2015), "This is not your mother's terrorism: social media, online radicalization and the practice of political jamming", *Journal of Terrorism Research*, 6(2), 1-16.

Séance 11 | 6 avril 2021 – Algorithmes, gouvernance et sécurité

Gouvernance des sujets, des flux et des mobilités à l'ère du Big Data et des algorithmes ; architecture, géographie et dynamiques des outils algorithmiques ; « machines numériques » et structuration de la sécurité, des individus, des mobilités et des flux.

Lectures :

- Aradau, C. & T. Blanke (2017), « Governing others: Anomaly and the algorithmic subject of security", *European Journal of International Security*, 3(1), pp. 1-21.
- Smith, Gavin JD (2020), "The Politics of Algorithmic Governance in the Black Box City", *Big Data & Society*, July-December: pp. 1-9.

Séance 12 | 13 avril 2021 – Technologie, pensée magique et enjeux éthiques
Réflexion sur le rôle et la place dans la technologie dans les politiques publiques en matière de sécurité ; effets pervers des technologies ; réflexion éthique ; discrimination et conséquences des biais de technologies.

Lectures :

- Morozov, Evgeny (2013), "Introduction" and "Solutionism and Its Discontents", in To Save Everything, Click Here. The Folly of Technological Solutionism, New York: Public Affairs, pp. vii-16.
- Seeta Peña Gangadharan & Jędrzej Niklas (2019), « Decentering technology in Discourse on Discrimination", *Information, Communication & Society*, 22(7), pp. 882-899.

20 avril 2021 | RMISE DU TRAVAIL FINAL – FORMAT WORD – 17H00

Bibliographie sélective :

Aas, K. F. ; Gundhus, H. O. & Lomell, H. M. (eds.) (2009), *Technologis of Insecurity*. London : Routledge.

Ball, K. ; Lyon, D. & Haggerty, K. (eds.) (2012), *The Routledge Handbook of Surveillance Studies*. London, New York : Routledge.

Benkler, Y. ; R. Faris & H. Roberts (2018), *Network propaganda : manipulation, disinformation, and radicalization in American politics*, New York : Oxford University Press.

Benjamin, R. (2019), *Race After Technology. Abolitionist Tools for the New Jim Code*. Cambridge: Polity.

Bennet, C. (2011), *Security Games*. New York : Routledge.

Boullier, D. (2016), *Sociologie du numérique*. Paris : Armand Colin.

Browne, S. (2015), *Dark Matters. On the Surveillance of Blackness*. Durham & Londres: Duke University Press.

Burgess, P. (2010). *The Routledge Handbook of New Security Studies*. New York : Routledge.

Cheney-Lippold, J. (2017), *We are data : algorithms and the making of our digital selves*. New York : New York University Press.

Crettiez, X., & Piazza, P. (dirs.) (2006), *Du papier à la biométrie : identifier les individus*. Paris : Les Presses de SciencesPo.

Ducol, B. (2015), A Radical Sociability : In defense of an off-line/on-line multidimensional approach to radicalisation, in Bouchard, M. (dir.), *Social Networks, Terrorism and Counter-Terrorism : Radical and Connected Account*. Londres : Routledge : 87-107.

Ellul, J. (1988), *Le bluff technologique*. Paris : Hachette.

Ellul, J. (1954), *La technique ou l'enjeu du siècle*. Paris : Armand Colin.

Evans, C. L. (2018), *Broad Band. The Untold Story of the Women Who Made the Internet*. Londres: Penguin.

Feenberg, A. (1999), *Questioning Technology*. Londres, New York: Routledge.

Grobois, P. (2018), *Les batailles d'Internet. Assauts et résistances à l'ère du capitalisme numérique*, Montréal : Écosociété.

Hargittai, E. & C. Sandvig (dirs.) (2015), *Digital research confidential : The secrets of studying behavior online*. Cambridge MA. : MIT Press.

Halpern, C. ; P. Lascoumes & P. Le Galès (2014), *L'instrumentation de l'action publique.* Paris : Les Presses de SciencesPo.

Huysmans, J. (2014). *Security Unbound. Enacting Democratic LImits*. London : Routledge.

Lupton, D. (2015), *Digital Sociology*. London & New York : Routladge.

Lyon, D. (2015), *Surveillance After Snowden*. Cambridge : Polity Press.

Marx, G. (2001), Technology and Social Control : The Seacrh for the Illusive Silver Bullet, in N. J.. Smelser & P. B. Balte (eds.), *International Encyclopedia of the Social and Bahavioural Sciences*. New York : Elsiver.

Manning, P. K. (2011). *The Technology of Policing*. New York : NYU Press.

Misa, T. J.; P. Brey & A. Feenberg (2003), *Modernity and Technology*. Cambridge, M. A.; Londres: The MIT Press.

Norris, C. & Armstrong, G. (1999). *The Maximum Surveillance Society : the Rise of CCTV*. Oxfrod : Berg.

Pötzsch, H. (2015), « The emergence of iBorder: bordering bodies, networks, and machines », *Society and Space*, 33, pp. 101-118.

Simondon, G. (1958), *Du mode d'existence des objets techniques*. Paris : Aubier.

Singer, P.W. & E. T. Brooking (2018), *Like War : The Weaponization of Social Media*. Boston, New York : An Eamon Dolan Book, Houghton Mifflin Harcourt.

Winner, L. (1977). *Autonomous Technology : Technics Out-Of-Control as a Theme in Political Thought*. Cambridge, MA. : New Press.

Zuckerberg, D. (2018), *Not All Dead White Men. Classic Misogyny in the Digital Age.* Cambridge, Londres: Harvard University Press.