SIP 3071 | QUESTION DE SÉCURITÉ INTÉRIEURE – TECHNOLOGIE, INFORMATION ET SÉCURITÉ

Plan de cours | Hiver 2021

Jeudi. 9h00-11h15 – Enseignement à distance | Zoom

Samuel Tanner – professeur agrégé
École de criminologie – Université de Montréal
Bureau C-4100 (Pavillon Lionel-Groulx)

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

Disponibilités : sur rendez-vous par courriel

Descripteur : séminaire permettant à l'étudiant d'approfondir certaines matières du domaine de la sécurité intérieure

1. Introduction

La technologie a connu un développement fulgurant ces dernières décennies et occupe une place centrale dans nos sociétés contemporaines, qu'il s'agisse du secteur de la sécurité, de l'éducation, de la santé ou de nos vies quotidiennes. Bien qu'historiquement ancrée dans nos vies, la technologie et les développements récents qui caractérisent son développement posent de nouveaux défis et enjeux sur les plans sociaux, politiques, juridiques et éthiques et méritent une attention particulière, y compris dans le champ de la sécurité.

La technologie peut s'appréhender sous l'angle de l'action publique, soit « l'action gouvernementale, l'action (collective) qui participe à la création d'un ordre social […], à la direction de la société, à la régulation de ses tensions, l'intégration des groupes et à la résolution des conflits » (Lascoumes & Le Galès, 2005 : 12). L'action publique relève de « l'ensemble des problèmes posés par le choix et l'usage des outils [des technologies] qui permettent de matérialiser et d'opérationnaliser l'action gouvernementale » (Lascoumes & Le Galès, 2005 : 12). La technologie s'envisage alors comme un instrument d'action publique, ou « dispositif à la fois technique et social qui organise les rapports sociaux spécifiques entre la puissance publique [les autorités, par exemple] et ses destinataires [les citoyens, par exemple] en fonction des représentations et des significations dont il est porteur » (Halpern, Lascoumes & Le Galès, 2014 : 17). Ce cadre s'avère utile pour penser le rôle de la technologie et de l'information en lien à la sécurité.

Aux prises avec des restrictions budgétaires et un manque chronique de ressources, les acteurs de la sécurité, particulièrement du secteur public, ont largement considéré la technologie comme étant une réponse nécessaire dans un contexte d'exigence et de pression accrue de résultats, tendant à croire que la technologie offre une solution à tout problème, phénomène mieux connu sous le nom de techno-solutionnisme. À titre d'exemple, les caméras portatives sur les policiers, la reconnaissance faciale, la police prédictive basée sur les Big Data et les algorithmes, sont désormais populaires. Or, si ces outils semblent a priori, et dans leur conceptualisation, offrir des solutions à des problèmes concrets (manque de transparence de la police, profilage) leur appropriation et les conséquences, ou effets, de leur utilisation s'accompagnent de sérieuses limites qui nécessitent une attention particulière de la part des décideurs. Dans les formes les plus préoccupantes de leurs déploiements, ces technologies accentuent la discrimination à l'égard de groupes.

Par ailleurs, les technologies de l'information, dont les plateformes numériques (Facebook, Twitter, Tik Tok) et sans lesquelles nos vies sociales et professionnelles seraient compromises, sont aussi des objets de préoccupation en matière de sécurité et de démocratie. Leur utilisation est préoccupante dans l'amplification de contenus problématiques, qu'il s'agisse de fausses nouvelles, mais aussi de haine ou de discours faisant la promotion de discriminations. De par leur fonctionnement et leur capacité à recommander des contenus problématiques, ces technologies exercent une influence sur les esprits et les opinions de la population en enfermant le public dans des communautés symboliques qui limitent l'accès à l'information essentielle pour exercer ses droits civiques. Enfin, et sans pour autant dresser ici une liste exhaustive des impacts de ces technologies en matière de sécurité, elles s'accompagnent de transformations importantes des rapports entre gouvernants et gouvernés. On pense par exemple au rôle des technologies portables, comme les cellulaires, dans la prise de vue dans les rues et l'impact de ce phénomène sur les acteurs de la sécurité, y compris la police (copwatching).

En conséquence, une réflexion sur le rôle des technologies en matière de sécurité dans nos sociétés contemporaines à travers un triple espace de réflexion (conceptualisation, appropriation et conséquences des technologies) s'avère cruciale compte tenu de leur rôle croissant en matière de sécurité.

2. Objectif général du cours

L'objectif de ce cours vise à initier les étudiants aux questions d'information, communication et technologies en lien à la sécurité intérieure. En particulier, il a pour objectif de développer des connaissances et une réflexion sur l'impact des nouvelles technologies employées de manière exponentielle en sécurité intérieure, qu'il s'agisse des technologies de surveillance, de prédiction, de régulation des flux informationnels ou de communication. À l'issue de ce cours, les étudiants disposeront de connaissances solides en lien à l'impact des technologies, de la communication et de l'information en matière de sécurité et seront en mesure de les appliquer à une technologie concrète, tant du point de vue de ses enjeux techniques, politiques, sociaux et juridiques.

3. Pédagogie et enseignement

Compte tenu du contexte actuel de pandémie de la COVID-19, et de la nécessité de maintenir des mesures sanitaires assurant la sécurité de toutes et tous, **le cours aura lieu exclusivement à distance sur Zoom les jeudis de 9h à 11h15, à partir du 14 janvier 2021**. Le lien Zoom sera communiqué sur la plateforme StudiUM du cours. La matière sera essentiellement donnée sous forme d'exposés magistraux synchrones et sous forme de capsules par le professeur. Cette méthode permettra l'acquisition des connaissances théoriques et empiriques nécessaires, ainsi qu'un bagage conceptuel indispensable pour atteindre les objectifs du cours ci-dessus explicités.

En dépit des contraintes de l'enseignement à distance, le professeur assurera un maximum d'interactions possibles avec les étudiant.e.s, afin de maintenir des séances les plus dynamiques possibles. Dans cet esprit, une partie de la matière sera donnée sous forme de capsules pour permettre davantage de discussions durant la séance. Ces capsules seront disponibles sur StudiUM une semaine avant la séance.

Afin de garder les échanges les plus agréables possibles, **les étudiant.e.s sont invité.e.s à maintenir leur caméra allumée lors des séances**. Pour faciliter l'apprentissage de la matière, chaque séance sera enregistrée et rendue disponible pour visionnement sur StudiUM dédié au cours (fichier audio). Afin de dynamiser les séances, les étudiant.e.s sont encouragé.e.s à poser des questions en tout temps, ainsi qu'à exprimer leurs opinions et/ou exposer leurs expériences durant les séances. Par ailleurs, et pour faciliter cette dynamique, **un forum** sera accessible à l'ensemble des participants du cours qui aura pour objectif de faciliter les échanges et la discussion (questions éventuelles sur la matière, les lectures ou le partage de ressources (p. ex. articles dans les médias, documentaire, film, etc.).

4. Évaluation

L'évaluation du cours s'organisera **en trois étapes.** Les consignes pour la réalisation de chacune des trois étapes, ainsi que de leur évaluation, vous seront communiquées dans les premières semaines de la session.

1. **Un commentaire** portant sur un enjeu d'actualité en lien à la technologie (30%) (3 pages). À remettre au plus tard le 26 février 2021.
2. Un **bulletin d'approfondissement** sur une notion, un concept ou un phénomène au choix vu durant le cours et que les étudiant.e.s souhaitent développer à titre individuel (30%). (3 pages). À remettre au plus tard le 9 avril 2021.
3. Un **travail final** portant sur une technologie au choix de l'étudiant.e. (40%) (10 pages). À remettre au plus tard le 16 avril 2021.

La notation des travaux se réalisera à partir du barème ci-dessous :

Grille de conversion des pourcentages			
Points	Note littérale	Valeur	Pourcentage
4,3	A+	Excellent	90
4	A		85
3,7	A-		80
3,3	B+	Très bon	77
3	B		73
2,7	B-		70
2,3	C+	Bon	65
2	C		60
1,7	C-		57
1,3	D+	Passable	54
1	D		50
0	E	Échec	-de 50

Il est à noter que les étudiants seront également évalués sur la qualité de la langue. Aussi, et pour ceux qui éprouveraient des difficultés à l'écriture et à la grammaire, il est recommandé de prendre contact avec le **Centre de communication écrite de l'Université de Montréal**. Ce service est gratuit pour tous les étudiants inscrits. Pour plus d'information, les personnes intéressées pourront consulter l'adresse suivante : www.cce.umontreal.ca

Le plagiat est sanctionné par le *Règlement Disciplinaire sur la Fraude et le Plagiat Concernant les Étudiants*. Tout plagiat se verra attribuer la note 0 et sera rapporté à la Faculté des Arts et sciences. Plagier peut entraîner un échec, la suspension ou le renvoi de l'université. Il est fortement recommandé de prendre connaissance des règles en vigueur à l'Université de Montréal en matière de plagiat. Ces règles sont accessibles en cliquant sur le lien suivant : www.integrite.umontreal.ca.

Enfin, les travaux remis en retard sans autorisation préalable du professeur seront pénalisés de 10% le premier jour, puis de 5% pour chaque jour subséquent. Ce délai ne peut dépasser 5 jours. Les jours de fin de semaine et les jours fériés comptent comme des jours réguliers.

!!!! IMPORTANT !!!!

Selon le règlement pédagogique (article 9.9 reproduit ci-dessous), l'étudiant doit motiver toute absence à une évaluation ; pour ce faire, **il faut s'adresser au Secrétariat de son département d'attache et non pas au professeur**. Seul un motif imprévu et hors du contrôle de l'étudiant peut être acceptable. Quand l'absence est motivée, l'étudiant sera informé par écrit des modalités de reprise de l'évaluation. La modalité de reprise des examens est la suivante : passer un examen différé (dans le cas d'un examen intra) OU passer un examen final cumulatif (qui porte sur toute la matière couverte durant la session) OU compléter un travail compensatoire. **Le choix de la modalité appartient à l'enseignant du cours**. En cas d'absence à un examen intra, la réussite d'un cours ne peut jamais se faire sur la base d'un examen final non cumulatif.

*« L'étudiant doit motiver, par écrit, toute absence à une évaluation ou à un cours faisant l'objet d'une évaluation continue **dès qu'il est en mesure de constater qu'il ne pourra pas être présent à une évaluation** et fournir les pièces justificatives. Dans les cas de force majeure, il doit le faire le*

plus rapidement possible par téléphone ou ***courriel et fournir les pièces justificatives dans les cinq jours ouvrables suivant l'absence****.*

Le doyen ou l'autorité compétente détermine si le motif est acceptable en conformité des règles, politiques et normes applicables à l'Université.

Les pièces justificatives doivent être dûment datées et signées. De plus, ***le certificat médical doit préciser les activités auxquelles l'état de santé interdit de participer, la date et la durée de l'absence, il doit aussi permettre l'identification du médecin****.»*

5. Lectures, ressources obligatoires

Le cours nécessite une lecture obligatoire par séance. La séance 9, quant à elle, nécessite le visionnement d'un documentaire. **Ces ressources constituent matière à évaluation au même titre que l'information présentée lors des séances**. L'ensemble des textes sera disponible en format pdf sur le site StudiUM du cours. Il est à noter que StudiUM sera utilisé comme plateforme d'accès aux lectures obligatoires, aux capsules pré-enregistrées, au matériel pédagogique (PPT), au forum de discussion associé au cours, ainsi qu'à l'affichage des résultats des évaluations (anonymisés).

6. Calendrier des rencontres

Séance 1 | 14 janvier 2021 – Introduction et présentations
Présentation du plan de cours, présentation des uns et des autres, organisation de la matière et de la démarche pédagogique ; introduction aux notions d'information, technologie et leur rapport à la sécurité.

BLOC A – Conceptualiser les technologies et leur usage.

Séance 2 | 21 janvier 2021 – Perspective historique et conceptualisation de la technologie
Dimensions historique et conceptuelle de la technologie ; évolution du rapport à la sécurité (pouvoir politique et biopolitique) ; progression de la technologie : linéaire ou par à-coups ? ; réflexion à partir des technologies de délimitation de l'espace (barbelé).

Lecture :

- Razac, Olivier (2009), *Histoire politique du barbelé*, Paris : Flammarion, pp. 205-229.

Séance 3 | 28 janvier 2021 – Technologie, enjeux socio-politiques et justice sociale
Enjeux socio-politiques entourant la conceptualisation et l'espace de formulation/élaboration de la technologie ; effets pervers et conséquences de l'usage de la technologie ; éthique, technologie et discrimination ; technologie et sécurité comme bien commun.

Lecture :

- Benjamin, Ruha (2019), Engineered Inequality: Are Robot Racist? in *Race After Technology: Abolitionist Tools for the New Jim Code*, Cambridge: Polity: 49-76.

Séance 4 | 4 février 2021 – Humains, technologies et cyborgs

Appropriation de- et résistance à la technologie ; rapport entre humains et technologie ; approche socio-technique de l'usage de la technologie ; « matérialité » de la technologie ; échange de propriétés entre humains et technologie ; une étude de cas de l'(h)acktivisme de droite radicale.

Lecture :

- 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.

BLOC B : Technologie et contrôle social

Séance 5 | 11 février 2021 – Mouvements sociaux, technologies et contrôle social

Mouvements sociaux, activisme et technologie ; rôle de la technologie et des plateformes numériques dans la mobilisation des acteurs et des idées ; neutralisation stratégique, technologie et contrôle des foules.

Lecture :

- Dumitrica, Delia & Mylynn Felt (2020), « Mediated Grassroots Collective Action: Negotiating Barriers of Digital Activism", *Information, Communication & Society*, 23(13): pp. 1821-1837.

Séance 6 | 18 février 2021 – Police, technologie et « copwatching »

Utilisation de la technologie par la police ; surveillance et technologie ; transformation des rapports entre gouvernants et gouvernés ; copwatching / sous-veillance ; impact de la prise d'image dans l'espace public.

Lecture :

- Meyer, Michaël & Samuel Tanner (2017), « Filmer et être filmé : La nouvelle visibilité policière à l'ère de la sousveillance », *Réseaux*, 201, pp. 175-205.

BLOC C – Information et sécurité

Séance 7 | 25 février 2021 – Information, technologie, démocratie et sécurité (1)

Information et enjeux de sécurité dans nos démocraties ; écosystème médiatique, nature et fonctionnement des plateformes numériques ; biais cognitifs ; boulimie de l'information ; influence et fabrique des opinions.

Lecture :

- Bronner, Gérald (2013), « Lorsque plus, c'est moins : massification de l'information et avarice mentale », in *La démocratie des crédules*. Paris : PUF, pp. 21-54

26 février 2021 | Date de remise du commentaire (30%)

Séance 8| 11 mars 2021 – Information, technologie, démocratie et sécurité (2)
Formes particulières et impacts de « déviances » de l'information ; information comme « arme de distraction massive » ; contexte « post-vérité » ; « fake news » ; « cheap / deep fakes » ; propagande computationnelle ; technologie comme amplificateur et accélérateur de l'infodémie ; activisme et information.

Lecture :

- Wooley, Samuel (2020), « chap. 5: Fake Video: Fake, but not yet Deep", in *The Reality Game: How the Next Wave of Technology Will Break the Truth*, New York: Public Affairs. pp. 107-130.

Séance 9 | 18 mars 2021 – Réguler l'information : enjeux et débats
Régulation de l'information et démocratie ; politique de l'information ; outils technologiques et juridiques de régulation de l'information ; stratégie de régulation et modération du contenu ; acteurs humains et non-humains de la régulation.

Documentaire / source média :

- Riesewieck, Moritz & Hans Block (2018), *The Cleaners.* Berlin: I wonder Pictures.
  (disponible sur Kanopy via le VPN UdeM)

BLOC D – Big Data, intelligence artificielle et sécurité

Séance 10 | 25 mars 2021 – Sécurité, Big Data et algorithmes : police prédictive
Police, intelligence artificielle et big data : nouveaux modèles policiers et lutte contre la criminalité ; sécurité et algorithme ; technologie et prédiction de la délinquance ; police prédictive et application de la loi guidée par les données.

Lecture :

- Benbouzid, Bilel (2018), « Quand prédire c'est gérer : la police prédictive aux États-Unis », *Réseaux*, 211(5), pp. 221-256.

Séance 11 | 1er avril 2021 – Technologie, quantification de soi, contrôle social et surveillance
Données personnelles et capitalisme de la surveillance ; exploitation des traces numériques et données personnelles en matière de sécurité ; cadre juridique et protection des données personnelles ; surveillance à l'ère de la quantification et exposition de soi.

Lecture :

- Dagiral, Éric, Christian Licoppe, Olivier Martin & Anne-Sylvie Pharabord (2019), Le quantified self en question(s) : un état des lieux des travaux de sciences sociales consacrés à l'automesure des individus. *Réseaux*, 216(4) : 17-54.

Séance 12 | 8 avril 2021 – Surveillance et reconnaissance faciale

Accélération et développement des technologies biométriques et de reconnaissance faciale ; enjeux et débats en lien à la sécurité et à la protection des données ; dimensions légale, éthique et politique ; enjeux technologiques et sociaux.

Lecture :

- Castets-Renard, Céline & Émilie Guiraud (2020), *Cadre juridique applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada : éléments de comparaison avec les États-Unis et l'Europe*. Observatoire International sur les Impacts Sociétaux de l'IA et du Numérique – OBVIA, Québec, pp. 14-55.

9 avril 2021 | Date de remise du bulletin (30%)

16 avril 2021 | date de remise du travail final (40%)

Références

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

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

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.

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

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

Benbouzid, B. (2018), « Quand prédire c'est gérer. La police prédictive aux États-Unis », *Réseaux*, 211(5), pp. 221-256.

Cardon, Dominique (2019), *Culture numérique*. Paris : Les Presses SciencesPo.

Cardon, Dominique (2015), *À quoi rêvent les algorithmes ? Nos vies à l'heure des big data*. Paris : Seuil.

Cardon, Dominique (2010), *La démocratie Internet*. Promesses et limites. Paris : Seuil.

Ceyhan, A. (2006). « Enjeux d'identification et de surveillance à l'heure de la biométrie ». *Cultures & Conflits*, 64 : 33-47.

Chan, J. (2001). « The technological game: How information technology is transforming police practice ». *Criminal Justice*, 1(2): 139-159.

Howard, Philip. N. (2020), *Lie Machines. How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. New Haven, Londres: Yale University Press.

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.

Loveluck, Benjamin (2016), « Le vigilantisme numérique, entre dénonciation et sanction. Auto-justice en ligne et agencements de la visibilité», *Politix* 115(3), pp. 127-153.

Morozov, Evgeny (2013), *To Save Everything, Click Here. The Folly of Technological Solutionism*. New York: Public Affairs.

O'Neil, Cathy (2018), *Algorithmes: la bombe à retardement*. Paris : Les Arènes.

Pasquale, Frank (2015), *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge, Londondres: Harvard University Press.

Roberts, Sarah T. (2019), *Behind the Screen. Content Moderation in the Shadows of Social Media*. New Haven, Londres: Yale University Press.

Tufekci, Zeynep (2017), *Twitter and Tear Gas. The Power and Fragility of Networked Protest*. New Haven, Londres: Yale University Press.

Wooley, Samuel C. & Philip N. Howard (2019), *Computational Propaganda. Political Parties and Political Manipulation on Social Media*. New York: Oxford University Press.