**SIP 3082 | TECHNOLOGIE, INFORMATION ET SÉCURITÉ**

**Plan de cours | Automne 2023**

**Mardi. 15h30-18h30**

**Samuel Tanner – professeur titulaire**
**École de criminologie – Université de Montréal**
**Bureau C-4128 (Pavillon Lionel-Groulx)**

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

**Disponibilités : sur rendez-vous par courriel**

**Descripteur** : Information, communication et technologies en lien avec la sécurité intérieure. Impacts de technologies en sécurité intérieure. Enjeux politiques, sociaux et historiques de la technologie en sécurité. Facteur humain et technologie de sécurité.

## 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 ancrés 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. Ils 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 ainsi 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, mais pas uniquement] 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, considèrent souvent la technologie comme un moyen nécessaire dans un contexte d'exigence et de pression accrue de résultats. En cela, la technologie offrirait une solution de choix à de nombreux problèmes, 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 (par ex. 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. Également, et sans pour autant prétendre à l'exhaustivité 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).

Par ailleurs, les technologies de l'information, et en particulier les plateformes numériques mues par l'intelligence artificielle (*Facebook, X, TikTok*), désormais totalement intégrées dans nos vies sociales et professionnelles, posent tout autant des questions en termes 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 et de désinformation. Étant donné leur fonctionnement et leur capacité à recommander des contenus problématiques, ces technologies exercent une influence majeure sur le marché des idées et sur les esprits et les opinions de la population en enfermant le public dans des communautés symboliques qui limitent l'accès à l'information, pourtant essentielle à l'exercice des droits politiques et civiques. En cela, elles présentent le risque de perturbation de la démocratie.

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 du cours vise à initier les étudiant.e.s 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 étudiant.e.s disposeront de connaissances solides en lien à l'impact des technologies, de la communication et de l'information en 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

**Le cours se déroule le mardi de 15h30 à 18h30 dans la salle B-3562 à partir du 5 septembre 2023.** La matière sera essentiellement donnée sous forme d'exposés magistraux 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. Le professeur assurera un maximum d'interactions possibles avec les étudiant.e.s, afin de maintenir des séances les plus dynamiques possibles. En retour, 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.

## 4. Évaluation

L'évaluation du cours s'organisera **en trois étapes.** Les consignes pour la réalisation de chacune de celles-ci, ainsi que de leur évaluation, vous seront communiquées dans les premières semaines de la session. Les travaux doivent être remis à l'adresse courriel du professeur.

1. **Un commentaire** portant sur un enjeu d'actualité en lien à la technologie (30%) (3 pages). À remettre au plus tard le 31 octobre 2023.
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 5 décembre 2023.
3. Un **travail final** portant sur une technologie au choix de l'étudiant.e. (40%) (10 pages). À remettre au plus tard le 19 décembre 2023.

En accord avec la politique de la Faculté des Arts et Sciences, l'utilisation de logiciels ou agents conversationnels utilisant l'IA (ex. ChatGPT, Bard, etc.) pour la réalisation d'une évaluation est strictement interdite. À cet égard et selon l'article 1.2 du Règlement disciplinaire sur le plagiat ou la fraude concernant les étudiants du premier cycle :

> *« Constitue notamment un plagiat ou une fraude : […] o) l'utilisation totale ou partielle, littérale ou déguisée d'un texte, d'un tableau, d'une image, d'un exposé, d'un enregistrement ou de toute autre création, généré[s] par un système d'intelligence artificielle, à moins d'autorisation explicite à l'occasion d'une évaluation »*

Cependant, les outils d'Intelligence artificielle (IA générative, ChatGPT, Bard, etc.) **peuvent faire l'objet d'une analyse critique** dans le cadre d'un travail comptant comme évaluation (ex. compréhension de la plateforme, critique de son fonctionnement, biais, analyse de leur production, etc.). Pour cela, les étudiant.es doivent clairement indiquer qu'ils font usage d'un tel outil et celui-ci doit être clairement référencé dans le travail. Pour cela, le site web des Bibliothèques de l'UdeM propose des modèles pour citer des sources comme ChatGPT (voire section 13.3). Dans le doute il est recommandé de s'entendre avec le professeur au préalable.

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 étudiant.e.s seront également évalué.e.s sur la qualité de la langue. Aussi, et pour celles et 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 : https://vieetudiante.umontreal.ca/soutien-etudes/connaissance-francais

**Le plagiat est sanctionné** par le *Règlement Disciplinaire sur la Fraude et le Plagiat Concernant les Étudiants*. Tout plagiat 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 : https://integrite.umontreal.ca/accueil/

**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. **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, au matériel pédagogique (PPT), ainsi qu'à l'affichage des résultats des évaluations (anonymisés).

## 6. Calendrier des rencontres

**Séance 1 | 5 septembre 2023 – Introduction et présentations**
Présentation du plan de cours, présentation des un.es 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 | 12 septembre 2023 – 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 | 19 septembre 2023 – 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 | 26 septembre 2023 – Rapports entre humains et technologies**
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 illustration l'utilisation des plateformes numériques dans le cadre d'opposition aux mesures sanitaires.

***Lecture :***

- Tanner, Samuel & Aurélie Campana (2022), « Je ne suis pas anti-vaccin, mais cette affaire de COVID-19 pue la merde ». La fabrique du discours opposé aux mesures sanitaires dans la Twittosphère canadienne. *Criminologie*, 55(2) : pp. 269-294.

**BLOC B : Technologie, participation sociale et contrôle social**

**Séance 5 | 3 octobre 2023 – Mouvements sociaux, participation citoyenne et technologies**
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 | 10 octobre 2023 – Police, technologie, médias et contrôle social**
Utilisation de la technologie par la police ; surveillance et technologie ; participation des citoyens dans la gouvernance de la sécurité ; visibilité, médias et police ; rapports entre gouvernants et gouvernés ; copwatching / sous-veillance ; impact de la prise d'image dans l'espace public.

***Lecture :***

- Ellis, Justin R. (2023), « Social media, police excessive force and the limits of outrage: Evaluating models of police scandal". *Criminology and Criminal Justice*, 23(1): pp. 117-134.

**BLOC C – Information et sécurité**

**Séance 7 | 24 octobre 2023 – Information, technologie, démocratie et sécurité**
Information et enjeux de sécurité dans nos démocraties ; communauté épistémique ; marché de l'information et des idées ; écosystème médiatique, nature et fonctionnement des plateformes numériques ; 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

**31 octobre 2023 | Date ultime de remise du commentaire (30%)**

**Séance 8| 31 octobre 2023 – Information, intelligence artificielle (IA) et démocratie**
Intelligence artificielle ; participation sociale ; (dés)information ; contexte « post-vérité » ; logique algorithmique et propagande computationnelle ; ingérences étrangères ; économie de la désinformation ; mécanismes psychosociaux de la désinformation.

***Lecture :***

- Barela, Steven, J. & Jérôme Duberry (2021), "Understanding Disinformation Operations in the Twenty-First Century", in Hollis, Duncan B. & Jens David Ohlin (Dirs.), *Defending democracies: combatting foreign election interference in the digital age.* New York, NY: Oxford University Press, pp. 41-71.

**Séance 9 | 7 novembre 2023 – Réguler l'information à l'ère de l'IA**
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.

***Lecture:***

- Badouard, Romain & Margueritte Borelli (2023), "Réseaux sociaux et régulation des contenus : un enjeu de politique internationale », in Académie des sciences morales et politiques (Dir.), *Annuaire français des relations internationales*, Paris : Éditions Panthéon-Assas, pp. 875-886

**BLOC D – Big Data, intelligence artificielle, système de justice et sécurité**

**Séance 10 | 14 novembre 2023 – Sécurité, Big Data, algorithmes et prédiction**
Système de justice, 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 :***

- Ugwudike, Pamela (2022), "Predictive Algorithms in Justice Systems and the Limits of Tech-Reformism", *International Journal for Crime, Justice and Social Democracy,* 11(2): pp. 85-99.

**Séance 11 | 21 novembre 2023 – 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 | 28 novembre 2023 – 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.

**Séance 13 | 5 décembre 2023 : disponibilité du professeur pour le travail final (1heure)**

**5 décembre 2023 | Date ultime de remise du bulletin d'approfondissement (30%)**

**19 décembre 2023 | date ultime de remise du travail final (40%)**

**Références (sélection)**


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

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

Biondi, C. (2022), Dé-coder. *Une contre-histoire du numérique.* Paris : Bouquins Édition.

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

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

Brubaker, R. (2023), *Hyperconnectivity and Its Discontents*. Cambridge, UK; Hoboken, NJ: Polity.

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.

Crawford, K. (2021), *Atlas of IA. Power, Politics and the Planetary Costs of Artificial Intelligence.* New Haven & Londres: Yale University Press.

Da Empoli, G. (2023), *Les ingénieurs du chaos*. Paris : Gallimard, Folio.

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

Gerbaudo (2019), *The Digital Party. Political Organisation and Online Democracy*. Londres: Pluto Press.

Gillespie, T. (2018), *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. New Haven & London: Yale University Press.

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

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.

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

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

Noble, S. U. (2018), *Algorithms of Oppression. How Search Engines Reinforce Racism*. New York: New York University Press.

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.

Schick, N. (2020), *Deep Fakes. The Coming Infocalypse*. New York, Boston: Twelve.

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

Sustein, C. R. (2017), *#Republic. Divided Democracy in the Age of Social Media*. Princeton & Oxford: Princeton 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.