Direction scientifique de la collaboration
avec les acteurs publics, Obvia

Dans l'œil
de l'Obvia

FÉVRIER 2026

Surveillance augmentée par les nouvelles technologies : de l'exception à la norme

Mise en contexte

Quelques semaines après ses révélations en 2013 sur les opérations massives de surveillance en ligne de la part du gouvernement américain, Edward Snowden avait expliqué ses motivations ainsi : « Je ne veux pas vivre dans un monde où il n'y a pas de vie privée et donc pas de place pour l'exploration intellectuelle et la créativité »[1]. Treize ans plus tard, les technologies comme l'IA ayant évolué à un niveau sans précédent, les craintes chez certains experts de voir des gouvernements ou des forces de l'ordre abuser de leurs nouvelles capacités de surveillance sont bien réelles.

Pourtant, les sociétés semblent avoir accepté, de manière générale, les dispositifs numériques qui s'immiscent dans la vie privée : des caméras de surveillance sur les portes de nos voisins, des applications qui tracent le trajet exact d'une course à pied, des téléphones intelligents ou assistants vocaux qui semblent « écouter » nos conversations pour nous proposer de la publicité[2], etc. Serions-nous plus à l'aise avec la collecte de nos données par des entités privées qu'avec la surveillance gouvernementale ou policière? À quel point ces deux activités sont-elles réellement distinctes l'une de l'autre?

Cette note de breffage vise à offrir des pistes de réponse à ces questions et à faire le point sur les enjeux liés aux formes de surveillance augmentées par les algorithmes et les IA. En particulier, la note s'intéresse aux dispositifs de vidéosurveillance algorithmique, aux justifications de leur nécessité et à ce que leur utilisation peut entraîner comme dérives ou empiètements sur le droit à la vie privée.

Les informations présentées dans la note proviennent entre autres des échanges ayant eu lieu lors de la conférence *Technopolice : La surveillance policière à l'ère de l'intelligence artificielle*, présentée le 6 février 2026 dans le cadre du Cercle de lecture de l'axe Droit, cybersécurité et cyberjustice de l'Obvia.

Définition

La vidéosurveillance algorithmique ou augmentée (VSA) « [s'appuie] sur le parc de caméras de vidéosurveillance existant et "l'augmente" en proposant l'accès à des modèles d'intelligence artificielle (IA), qui fournissent une analyse automatisée des images, ainsi qu'à une interface dédiée à l'utilisateur (agent de sécurité, policier ou vidéo-opérateur), lui permettant de vérifier l'analyse. »[3]

1 Greenwald, G., MacAskill, E. et Poitras, L. (2013, 11 juin). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [traduction libre]
2 Ovide, S. (2025, 7 janvier). Is your phone listening to you? Yeah, but probably not to target ads. *The Washington Post*. https://www.washingtonpost.com/technology/2025/01/07/phone-listening-target-ads-iphone-siri/
3 Le Ludec, C. et Cornet, M. (2025). Qui rend lisibles les images ? L'intelligence artificielle au fondement d'une recomposition du travail de surveillance. Réseaux, 251(3), 113-144. https://doi-org.acces.bibl.ulaval.ca/10.3917/res.251.0113. p. 113

Résumé des connaissances

La ville connectée et son image sécuritaire

La vague mondiale de projets de modernisation des infrastructures municipales dans les années 2010 (dites « villes connectées » ou *smart cities*) a ouvert la porte à des refontes des systèmes de surveillance utilisés par les services de police pour les rendre plus performants. Le terme « ville sécuritaire » (*safe cities*) est donc apparu sans grande controverse et évoquant un sentiment de protection contre des méfaits et du terrorisme chez les citoyens et citoyennes. De nombreux chercheurs critiquent toutefois cette terminologie en raison de ses promoteurs, qui esquisseraient « une vision quasi apocalyptique de la ville pour mieux légitimer la solution technosécuritaire proposée, une rhétorique de la rédemption par la technologie »[4]. Le problème du **technosolutionnisme** serait ici à l'avant-plan. Notons par exemple qu'à Paris, en amont des Jeux olympiques (JO) de 2024, **« l'instrumentalisation de cet événement et de sa dimension exceptionnelle pour la mise en œuvre de mesures et de politiques technosolutionnistes a engendré des impacts sociaux considérables »**[5].

D'autres font valoir que l'étiquette de la ville connectée sécuritaire suggère aussi « une réalité floue, construite et conceptualisée principalement par les acteurs privés du marché de la sécurité »[6].

« Le marché mondial de la reconnaissance faciale augmente de 16 % par an et devrait atteindre 12 milliards de dollars en 2028 ; celui de la VSA était de 5,6 milliards en 2023 et pourrait représenter 16,3 milliards en 2028. »[7]

Avec de tels profits possibles pour les compagnies qui fournissent des dispositifs de VSA, il convient de s'interroger sur les réels moteurs de cette transformation des méthodes de sécurisation des lieux publics. L'exemple de la ville de Marseille, qui a dépensé des dizaines de millions d'euros pour l'installation de 500 nouvelles caméras de sécurité en 2018, est décrié sur deux plans : d'une part puisque l'estimation initiale du projet était trois fois moins coûteuse, d'autre part parce que la ville aurait des besoins criants dans une multitude d'autres sphères et que l'urgence d'installer ces caméras n'était pas prouvée[8].

La surveillance imbriquée dans le quotidien

Et si la surveillance policière était rendue possible par nos propres activités et habitudes de consommation? À Trois-Rivières, un registre de plus de 760 caméras de « sonnettes intelligentes » permet au service de police d'accéder à des images sur demande pour faciliter les enquêtes[9]. Puisque l'adhésion au registre est volontaire et qu'il est dans l'intérêt de la population que la police parvienne à résoudre des crimes, l'**acceptabilité sociale** du projet semble forte à ce stade-ci. Des chercheurs comme Vincent Gautrais et Pierre Trudel signalent toutefois que les garanties ne sont pas suffisantes que la police ne fera pas un usage abusif de ces images ou que ces dernières puissent tomber dans les mains d'autres parties[10].

Un autre objet de consommation peut représenter une porte d'entrée importante pour l'accès à nos données privées : la voiture. Les véhicules électriques, mais plus largement tous les véhicules connectés, amassent des quantités faramineuses de données sur les habitudes de ses occupants. Dans une enquête de la Mozilla Foundation de 2023, sur 25 fabricants automobiles évalués :

84 %
vendent ou partagent les données personnelles des usagers, sans consentement explicite

92 %
ne permettent peu ou pas de contrôle aux usagers sur leurs données personnelles

56 %
affirment pouvoir partager les données avec les forces de l'ordre en réponse à une requête informelle (et non une ordonnance de la Cour)[11].

Sujet d'actualité avec une flotte de véhicules électriques chinois qui fait son entrée au Canada, selon Guillaume Beaumier, l'enjeu ne serait pas la provenance du véhicule, mais bien l'encadrement juridique lacunaire au Canada, le gouvernement fédéral n'ayant pas mis sa législation sur la protection de la vie privée depuis 2001[12].

4 Tréguer, F. (2024). *Technopolice : La surveillance policière à l'ère de l'intelligence artificielle.* Divergences. https://shs-cairn-info.acces.bibl.ulaval.ca/technopolice--9791097088729?lang=fr. p. 64
5 Al Baba Douaihy, S., Loiseau, H. et Tardif, P.-M. (2025). *Le facteur humain, maillon fort de la cybersécurité des grands événements : le cas des Jeux olympiques et paralympiques de Paris 2024.* Obvia. https://doi.org/10.61737/CAER2957, p. 80
6 Challier, R., Picaud, M. et Castagnino, F. (2025). De la « safe city » aux dispositifs numériques de sécurité urbaine. *Réseaux*, 251(3), 11-43. https://doi-org.acces.bibl.ulaval.ca/10.3917/res.251.0011. p. 11
7 Tréguer, F. (2024) *op.cit.*, p. 50
8 Tréguer, F. (2024) *op.cit.*, p. 15
9 Arcand, F. (2026, 27 janvier). Sonnettes intelligentes contre le crime. *La Presse.* https://www.lapresse.ca/actualites/trois-rivieres/sonnettes-intelligentes-contre-le-crime/2026-01-27/qr/que-disent-les-experts-en-vie-privee.php
10 *Ibid.*
11 Caltrider, J., Rykov, M. et MacDonald, Z. (2023). *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy.* https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/
12 Beaumier, G. (2026, 11 février). Véhicules électriques chinois : le faux débat de la sécurité nationale. *Options Politiques.* https://policyoptions.irpp.org/fr/2026/02/vehicules-electriques-chinois/

Des zones d'essai pour propulser la VSA

L'implantation de nouvelles techniques de vidéosurveillance dans les différentes villes est rendue possible en partie grâce aux expérimentations, comme des projets pilotes, qui sont menés à plus petite échelle ou ailleurs dans le monde. La ville de Nice a par exemple testé un système de reconnaissance faciale lors de son carnaval en 2019 :

> **« Informées par des panneaux, 5 000 personnes avaient accepté de jouer le jeu en rentrant dans la zone dédiée à l'expérimentation, donnant ainsi une sorte de consentement censé abriter la ville sur le plan juridique. »**[13]

Le fournisseur israélien, par ailleurs, avait d'abord testé ses algorithmes dans les territoires palestiniens occupés. Un autre projet français a bénéficié de zones d'essais outre-mer : après un refus de la Commission nationale de l'informatique et des libertés (CNIL) de tester un algorithme de suivi d'individus recherchés (mais sans reconnaissance faciale) en sol français, le ministère de l'Intérieur a conclu, en 2018, une entente avec le gouvernement de Singapour pour mener cette expérimentation dans la cité-État[14]. Il y a donc un enjeu éthique clair lorsque l'implantation de la VSA dans nos sociétés nécessite l'exploitation de territoires où la juridiction est moins sévère face au droit à la vie privée, notamment puisqu'elle évoque des logiques coloniales.

Une autre façon de procéder est le recours aux « bacs à sable réglementaires ». Encouragés dans le Règlement européen sur l'IA (*AI Act*) et utilisés par le gouvernement du Canada[15], ils permettent une **dérogation temporaire aux lois en vigueur** pour tester des dispositifs, évaluer leurs résultats et leurs impacts et mesurer l'acceptabilité sociale. Initialement promues dans le secteur privé, ces zones d'expérimentation sont justifiées dans le discours entourant la réglementation de l'IA par la possibilité qu'elles offrent de vérifier que les prototypes respectent les lois en vigueur. D'autres font valoir qu'elles servent davantage d'outil de légitimation pour les technologies controversées[16].

Les grands évènements représentent aussi une forme de bac à sable pour la mise à l'essai de nouveaux outils de surveillance. Avant les JO de Paris en 2024, une loi a été adoptée afin d'élargir les pouvoirs policiers et permettre l'expérimentation de la vidéosurveillance algorithmique (article 10 de la loi du 19 mai 2023). Cette disposition interdisait néanmoins le recours à l'identification biométrique, au traitement de données biométriques et à la reconnaissance faciale[17]. Des critiques, notamment de la société civile, ont été émises tant par rapport aux coûts de cette expérimentation que face au **« développement de la surveillance de masse par une couche logiciel ajoutée à la vidéosurveillance »**[18]. Rappelons aussi que, déjà aux Jeux de Londres de 2012, 500 000 caméras de vidéosurveillance avec un logiciel de reconnaissance faciale dans les espaces publics de la ville avaient été installées[19].

Le travail policier lui-même transformé

L'ajout de dispositifs technologiques aux méthodes de travail des corps policiers a diverses répercussions sur le quotidien des agents. Le port de la **caméra corporelle**, par exemple, a été encouragé dans l'histoire récente comme une mesure permettant de protéger les citoyens d'un usage excessif de la force et pour renforcer la preuve dans les procédures judiciaires. Comme l'a remarqué le chercheur Félix Tréguer[(3)] lors d'une incursion dans le quotidien d'un policier américain, les agents sont tenus de suivre la procédure à la lettre lorsque la caméra est activée; une bonne chose a priori, cela les empêche de faire preuve de discernement dans des cas où une intervention plus humaine serait à envisager, sans fichage des individus comme le veut la formalité. Les policiers peuvent donc avoir l'impression d'obéir davantage aux impératifs technologiques qu'à leur propre jugement, en plus de se sentir surveillés par leurs supérieurs puisque divers dispositifs servent à évaluer la performance, comme le temps de réponse à un appel ou le quota d'arrestations[20].

Il existe aussi un risque que des agents ayant facilement accès à une banque d'informations personnelles **abusent de ces données sensibles**, par exemple avec le traçage d'une ex-conjointe ou la consultation du profil d'une personne connue. Même si une simple lecture injustifiée des fiches policières consiste déjà en un manquement éthique, un danger encore plus important est le partage ou la vente de ces informations à de tierces parties[21]. Globalement, les **exceptions pour les forces de l'ordre** dans les lois qui encadrent l'IA ou la protection des données personnelles renforcent ces risques.

13 Tréguer, F. (2024) *op.cit.*, p. 28
14 *Ibid.*, p. 38
15 Gouvernement du Canada (2025). *Politique sur les bacs à sable réglementaires.* https://www.canada.ca/fr/gouvernement/systeme/lois/developpement-amelioration-reglementation-federale/exigences-matiere-elaboration-gestion-examen-reglements/politique-bacs-sable-reglementaires.html#toc7
16 Tréguer, F. (2024) *op.cit.*, p. 171
17 Turci, A. (2025). *Cadre juridique des jeux Olympiques et Paralympiques de Paris 2024 : étude de la vidéosurveillance algorithmique.* Obvia. https://doi.org/10.61737/EUHZ7160, p. 18
18 *Ibid.*, p. 14
19 *Ibid.* p. 5
20 Tréguer, F. (2024) *op.cit.*, p. 131. À noter que les impacts du port de la caméra corporelle sont multiples et vont au-delà de cet exemple précis.
21 *Ibid.*, p. 112

Enjeux de transparence

L'opacité des projets et du marché de la surveillance peut menacer les droits fondamentaux des individus. En 2018, la Commission européenne a refusé de divulguer un rapport sur l'éthique d'un projet douanier visant la reconnaissance des émotions pour détecter des mensonges en « invoquant le secret commercial des entreprises du consortium »[22]. En ce qui concerne le **droit d'opposition**, il reposerait surtout sur le niveau d'information et de compréhension du public face aux dispositifs utilisés et aux possibilités de retrait. Aux JO de Paris, le rapport d'évaluation de l'article 10 sur l'expérimentation de la VSA a conclu que le public était insuffisamment informé de la mesure temporaire pour réellement pouvoir exercer son droit d'opposition[23].

Cette **invisibilisation** de la surveillance serait en soi une tactique pour adoucir son exercice, les individus l'acceptant simplement comme statu quo. En étant minimalement invasive, la surveillance devient une activité passive de collecte d'informations – souvent fournies involontairement[24].

Enfin, dans un contexte où la surveillance augmentée par l'IA est gourmande en fonds publics et présente de nombreux risques, la question de l'efficacité de ces systèmes s'impose. Le rapport déposé après les JO de Paris montre que les dispositifs n'ont pas été performants pour tous les types de détection prévus et qu'ils n'auraient pas été supérieurs à la détection par un humain. À cet effet, **« l'objectif de sécurisation des jeux [a] très principalement été rempli par une importante densité d'effectifs sur le terrain »**[25]. La Cour des comptes, en France, avait aussi statué en 2020 « qu'aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation »[26].

Rôles que peuvent jouer les acteurs publics

Renforcer la législation entourant le droit à la vie privée et la protection des données personnelles, par exemple en interdisant les transferts de données vers des pays dont le cadre réglementaire est encore plus laxiste[27]

Instaurer des balises strictes pour la consultation d'informations personnelles par les corps policiers, en la permettant seulement dans des conditions précises et en prévoyant des mesures disciplinaires et légales pour les abus

Exiger des études sur l'efficacité d'un dispositif de VSA avant son déploiement à grands coûts, pour évaluer si les résultats seraient en effet supérieurs à une surveillance principalement humaine

Toujours prévoir un contrôle humain sur les algorithmes utilisés dans le domaine de la surveillance, en y interdisant notamment la prise de décision automatisée

Lorsqu'une expérimentation ou un projet pilote de VSA est déployé, informer activement la population qui pourrait y être soumise, par exemple avec des affiches claires et pédagogiques, des points de presse et des canaux pour poser des questions et exercer son droit d'opposition

S'appuyer sur les recherches en sciences sociales pour mesurer les impacts de la VSA sur la population et ses implications éthiques avant de choisir d'y avoir recours et éviter d'instrumentaliser celles-ci pour donner une apparence d'acceptabilité sociale

22 *Ibid.*, p. 46
23 Turci, A. (2025) *op. cit.*, p.18
24 Voir Marx, G. T. (2016). *Windows into the Soul: Surveillance and Society in an Age of High Technology.* Chicago, London: University of Chicago Press. ISBN-13:978-0-226-28591-7
25 Turci, A. (2025) *op. cit.*, p.22
26 Tréguer, F. (2024) *op.cit.*, p. 119
27 Beaumier, G. (2025) *op.cit.*

Messages clés pour la politique et la pratique

1 La vidéosurveillance algorithmique (VSA) a été largement testée et déployée dans les dernières années, même dans des pays occidentaux où les droits à la vie privée et à la protection des données personnelles sont bien ancrés.

2 Les habitudes numériques des individus, allant de l'utilisation d'un ordinateur à la conduite d'une voiture moderne, alimentent des banques de données en informations personnelles qui pourraient être exploitées ultérieurement (incluant par les forces de l'ordre).

3 Différentes méthodes sont mobilisées pour faire accepter la VSA par une population, notamment la promesse de la ville connectée sécuritaire, l'expérimentation durant de grands évènements ou tout simplement l'invisibilisation de la surveillance.

4 La VSA doit encore faire ses preuves en termes de rapport coûts/bénéfices et l'accès aux données sensibles par des agents de police doit être mieux réglementé pour éviter des dérives ou des abus de pouvoir.

Pour aller plus loin

Consulter le rapport

Consulter le rapport

À vos agendas

2e édition du colloque de la direction Collaboration avec les acteurs publics de l'Obvia

La souveraineté numérique au Québec : concilier stratégie, éthique et intérêt public

15 avril 2026
En présentiel à Québec

Détails et inscription

Cette note a été réalisée en collaboration avec Benoît Dupont, professeur à l'École de criminologie de l'Université de Montréal et titulaire de la Chaire de recherche du Canada en cyberrésilience et de la Chaire de recherche en prévention de la cybercriminalité.

Découvrir l'axe Droit, cyberjustice et cybersécurité de l'Obvia

obvia

Pour nous contacter :

Observatoire international sur les impacts sociétaux de l'IA et du numérique

Pavillon Charles-De Koninck, local 2489
1030, avenue des Sciences-Humaines
Université Laval
Québec (Québec) G1V 0A6

collaboration@obvia.ca
418.656.2131 poste 401234

Pour en savoir plus

obvia.ca

Pour consulter les autres notes de breffage

https://doi.org/10.61737/QRUJ8768 ISBN : 978-2-925581-32-1