

•
je me protège de
la surveillance
des luminaires.



Je renforce ma
sécurité
Je protège ma vie
privée

“

Les éclairages urbains intelligents, souvent équipés de capteurs, caméras ou dispositifs de reconnaissance, soulèvent d'importants enjeux pour la vie privée des citoyens. En collectant des données sur les mouvements, les comportements ou la présence des individus dans l'espace public, ces systèmes peuvent créer un sentiment de surveillance permanente. Même si les données sont destinées à optimiser la consommation d'énergie ou à renforcer la sécurité, leur usage flou ou mal encadré peut entraîner des abus, une perte d'anonymat ou un détournement à des fins commerciales ou policières. Le manque de transparence sur la nature des informations collectées, leur durée de conservation et leur traitement renforce la méfiance des citoyens et pose des questions éthiques sur le respect des libertés individuelles dans l'espace public.

”



6 points de vigilances

01a

**Collecte
excessive de
données**

Les
**lampadaires
intelligents**
peuvent être
équipés de :

- Caméras de surveillance
- Capteurs audio (détection de bruits suspects, conversations)
- Capteurs de mouvements ou de présence
- Microphones
- Capteurs environnementaux (pollution, température, etc.)
- Antennes 5G ou Wi-Fi (suivi de connexions d'appareils mobiles)

Risque Ces capteurs peuvent collecter des données personnelles ou comportementales (présence, trajets, voix), parfois sans le consentement explicite des personnes.

02a

**Surveillance
de masse**

Si les données
sont transmises
en **temps réel** à
des **autorités** ou
entreprises
privées :

- Suivi des déplacements individuels
- Analyse des comportements dans l'espace public
- Profilage à grande échelle

Risque Cela peut mener à une forme de surveillance constante, réduisant l'anonymat dans l'espace public.

03a

**Analyse
automatisée**

Certaines **villes**
utilisent des
algorithmes
d'IA, de la
reconnaissance
faciale, etc.
pour :

- Détecter des comportements suspects
- Identifier des visages ou des plaques d'immatriculation

Risque Des erreurs, des biais algorithmiques ou une utilisation abusive peuvent entraîner des accusations injustes ou une discrimination.

04a

Faibles de sécurité

Les
**infrastructures
connectées**
peuvent être
piratées :

- Fuites de données personnelles
- Surveillance illégale
- Manipulation des capteurs

Risque Une mauvaise cybersécurité peut exposer les citoyens à des intrusions ou à des utilisations malveillantes de leurs données.

05a

Partage des données avec des tiers

**Les données
collectées**
peuvent être

- Vendues à des entreprises (marketing ciblé)
- Partagées avec des agences gouvernementales
- Stockées par des prestataires étrangers

Risque Les données peuvent sortir du contrôle des autorités locales, avec peu de transparence sur leur usage.

06a

Manque de transparence et de consentement

Souvent, les
citoyens ne sont
pas informés

- De la nature des capteurs
- De ce qui est enregistré ou stocké
- Des finalités réelles de la collecte

Risque Atteinte à la vie privée sans que les individus en soient conscients ou puissent s'y opposer.

Arrowhead est un projet technologique développé par **Indra, entreprise spécialisée dans les solutions technologiques et de défense**. L'un des aspects innovants du projet est l'usage de **caméras vidéo avec anonymisation automatique**. Voici comment cela fonctionne :

- **Captation vidéo en temps réel** via des caméras intégrées, souvent installées sur des infrastructures publiques (lampadaires, bâtiments, etc.).
- Les images captées sont **traitées localement ou en bordure de réseau (edge computing)** pour détecter des événements (mouvements suspects, incidents, etc.).
- **Anonymisation automatique** : les visages, plaques d'immatriculation, et autres données personnelles sensibles sont floutés ou masqués avant transmission ou stockage, pour respecter la vie privée des citoyens.



5 points de solutions

01b

Comprendre
ce qui est collecté

Informe-toi localement :

Consulte le site web de ta ville ou interroge les services municipaux sur les capteurs installés dans les lampadaires (caméras, micros, Wi-Fi, etc.).

Demande les politiques de confidentialité :

Certaines communes publient des chartes ou rapports sur les technologies urbaines.

02b

Limiter
son exposition

Évite les zones fortement surveillées quand c'est possible.

Désactive le Wi-Fi et le Bluetooth sur ton smartphone en déplacement : certains lampadaires collectent les adresses MAC des appareils connectés.

Utilise un téléphone avec des protections de confidentialité (iOS ou Android avec paramètres de sécurité renforcés).

03b

Exercer
ses droits

Au Québec (LPRPSP, CAI) et au fédéral (CPVP)
tu as le droit de demander :

- **Quels types de données** sont collectés
- **De t'opposer à la collecte** dans certains cas
- **D'accéder ou de faire supprimer** tes données
- **Tu peux écrire à la mairie** ou au responsable local du traitement des données (DPO).

04b

Utiliser des outils de protection numérique

Utilise un VPN sur ton téléphone pour masquer ta position réelle.

Utilise des applications de sécurité qui bloquent le suivi (comme DuckDuckGo Privacy Browser, NetGuard, Blokada).

Installe des outils de détection de surveillance Wi-Fi (comme Wigle WiFi ou WiGLE.net) pour savoir si des réseaux publics te traquent.

05b

Agir collectivement

Sensibilise les habitants à ces enjeux : plus de pression citoyenne = plus de transparence.

Demande un audit citoyen ou une charte de respect de la vie privée pour les technologies urbaines.

Rejoins ou contacte des associations de défense des libertés numériques (comme La Quadrature du Net, Privacy International, etc.).

En résumé



Action

Objectif

Désactiver Wi-Fi/Bluetooth	Réduire le pistage passif
S'informer sur les capteurs	Comprendre les risques
Exercer ses droits (RGPD)	Reprendre le contrôle
Utiliser un VPN / outils privacy	Masquer sa présence numérique
Militer localement	Faire évoluer les politiques

Pour toutes questions ou suggestions d'amélioration.

ubik-infosec.ca



[@michel-panouillot](https://www.linkedin.com/in/michel-panouillot)



A propos de l'auteur

Professionnel chevronné en sécurité de l'information, je cumule plus de dix ans d'expérience dans des environnements complexes et diversifiés, incluant les secteurs gouvernementaux, de la formation et militaire. Mon expertise est centrée sur l'analyse en cybersécurité, avec une spécialisation en gouvernance et conformité réglementaire.