



HAL
open science

Implémentation des technologies de sécurité au sein des organisations et sur la voie publique : répondre au succès des technologies de surveillance

Fabrice Lollia

► To cite this version:

Fabrice Lollia. Implémentation des technologies de sécurité au sein des organisations et sur la voie publique : répondre au succès des technologies de surveillance. Colloque Territoire(s) et sécurité(s) 2023, Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN); Université Gustave Eiffel, Apr 2023, Aix en Provence, France. hal-04075266

HAL Id: hal-04075266

<https://hal.science/hal-04075266v1>

Submitted on 4 Jun 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Implémentation des technologies de sécurité au sein des organisations et sur la voie publique : répondre au succès des technologies de surveillance

Lollia Fabrice, Docteur en sciences de l'information et de la communication
Fabricelollia@gmail.com

Introduction

Face au problème d'insécurité auquel sont confrontées les organisations, nombreuses sont celles qui ont choisi de mettre en place des systèmes visant à protéger leurs collaborateurs. En France, la loi a créé une réglementation relative à cette protection. Devant ce type de problématique, de nombreux outils technologiques de sécurité ont été conçus afin de répondre au besoin sécuritaire des entreprises et de leurs salariés. Plusieurs solutions sont en cours d'expérimentation. Des caméras de sécurité, par exemple, apparaissent au sein des organisations sous condition de respect d'une loi spécifique et sous surveillance permanente de la CNIL.

Aujourd'hui, avec le développement des technologies de l'information et de la communication, de nouveaux modes de protection sont disponibles pour les entreprises et leurs employés. La géolocalisation, par exemple, est un autre moyen utilisé par de nombreuses organisations pour protéger leurs collaborateurs, notamment lorsqu'elles sont installées dans des pays à risques où des pratiques telles que le kidnapping contre rançon sont courantes. Les organisations font face à un contexte de changement technologique qui évolue avec une rapidité impressionnante.

Dans la littérature scientifique, l'impact des technologies de sécurité est analysé de façon méthodique. Certains auteurs se focalisent sur les caméras (Diard), d'autres sur la géolocalisation (Lollia), d'autres encore sur les différents environnements dans lesquels s'inscrivent ces technologies. Certains étudient leur fonctionnement sur la voie publique (réf.), d'autres au sein des organisations et notamment des entreprises. Cependant, ces travaux ont tous un point commun : la sécurité des personnes et des biens. Il y a ainsi, pour les chercheurs, un espace à explorer concernant les perspectives communes liées à ces technologies de surveillance.

Le but de cet article est donc de tracer un cadre commun de l'environnement dans lequel évoluent ces technologies de sécurité. Il s'agit, en d'autres termes, de mettre en lumière les

facteurs communs qui influencent leur implémentation tant au sein des organisations que sur la voie publique.

Notre question de recherche sera donc la suivante : de façon globale, y a-t-il des facteurs qui influencent l'acceptation des technologies de sécurité dans les organisations et sur la voie publique ? Plus généralement, quels sont les critères permettant aux organisations comme aux entreprises d'assurer une bonne implémentation de ce type de technologie ?

Pour y répondre, nous utiliserons l'interdisciplinarité des sciences de l'information et de la communication en nous appuyant sur une perspective d'intelligence économique, comparative, constructiviste et interprétative. Cette analyse se base, d'une part, sur nos travaux en recherche-action dans le domaine des sciences de l'information et de la communication, concernant la protection d'organisations internationales (ambassade, consulat, groupe industriel), et, d'autre part, sur la littérature actuelle.

Nous commencerons par une brève revue de la littérature consacrée à ces nouvelles technologies, avant de voir quelles sont les difficultés qu'elles soulèvent et les résultats qu'elles offrent. Enfin, nous donnerons quelques recommandations à destination des praticiens.

Cet article intéressera aussi bien les chercheurs que les décideurs publics et privés. Il les guidera dans leur choix d'une technologie de sécurité dans le cadre privé (organisation/entreprise) ou public (commune/ville).

1. État de l'art : de la notion de surveillance à la notion d'acceptation des acteurs

A. De la surveillance...

L'un des problèmes posés par les technologies de surveillance telles que les caméras concerne les divergences de perception de celles-ci par les acteurs. Qu'elles soient implantées dans une organisation ou sur une voie publique, la réaction des usagers est toujours la même : ils ont peur d'être surveillés.

Que dit la littérature scientifique à ce sujet ? Selon le dictionnaire Larousse, le mot « surveillance » est formé de « sur » et de « veiller » et signifie globalement « veiller au-dessus de ». Il convient, en ce sens, de comprendre quel est le but de la surveillance sur les acteurs. La surveillance par des outils de sécurité tels que les caméras vise à modifier leur comportement. En effet, on suppose que ce regard technologique affectera les comportements déviants.

La littérature scientifique consacrée à la notion de surveillance s'appuie en partie sur le concept du panoptique de Bentham pour expliquer cet aspect. On le retrouve dans plusieurs expérimentations scientifiques afin d'expliquer les comportements des acteurs face à une technologie de surveillance. Par exemple, Servais et Devresse (2019) utilisent ce concept pour analyser l'ANPR au sein de la police. Les caméras dites ANPR flashent automatiquement les plaques d'immatriculation des véhicules sur la voie publique, qu'ils soient à l'arrêt ou en mouvement.

Lollia (2019), quant à lui, reprend également ce concept pour analyser le comportement des acteurs face à une technologie de sécurité (la géolocalisation) en milieu hostile. Au problème de la surveillance s'ajoute donc celui de la traçabilité.

Le panoptique est un concept de Jeremy Bentham qui représente une prison à l'architecture circulaire. Au centre de celle-ci, la présence d'un unique gardien est utilisée dans une logique économique afin de surveiller l'ensemble des prisonniers. Un jeu d'ombres et de lumières fait que les détenus n'ont pas besoin d'être surveillés. Par conséquent, ils ont l'illusion d'être surveillés de façon continue. Le gardien est alors perçu comme un pouvoir invisible mais en même temps qui voit tout. C'est ce pouvoir invisible qui permet le contrôle des prisonniers.

Cette théorie est en rapport direct avec les peurs liées aux nouvelles technologies de surveillance. La population et les employés craignent effectivement ce contrôle social invisible que celles-ci impliquent. De plus, ces outils ont de nombreuses limites, comme on peut le voir en Chine, ce qui renvoie à la théorie de Foucault évoquant des sociétés disciplinaires où la technologie exerce une forme de pouvoir et de contrôle (Bert, 2012).

Toutes ces théories sont désormais largement appliquées aux nouvelles technologies, notamment par des auteurs comme Laetitia Schweitzer (Schweitzer, 2011), qui développe la notion de panoptique assisté par ordinateur pour décrire la prison dans laquelle vit la société moderne.

Les théories postpanoptiques continues ont ensuite émergé, et dans leur lignée, les travaux de (Haggerty & Ericson, 2000) concernant la surveillance sont éclairants, avec la notion de « data double ». Ce concept montre que finalement, dans la société contemporaine, l'individu est dématérialisé virtuellement et remonté, voire retracé à partir de séquences d'informations fournies par ces données.

Aujourd'hui, les visions de la surveillance de Foucault sont vivement critiquées, car elles ne correspondent plus à la société moderne. Les recherches apportent désormais des points de vue différents, à l'instar de Haggerty et Ericsson, par exemple, ou encore de Deleuze avec le concept de « sous-veillance ». Si la surveillance est par définition le fait de « veiller au-

dessus », la « sous-veillance » serait le fait de « veiller en dessous », de façon discrète, légère, immatérielle et omniprésente.

Aujourd'hui, en France, de nombreuses organisations et de plus en plus de communes de moins de 10 000 habitants sont équipées de caméras de surveillance. Pour autant, doit-on y voir un signe d'efficacité ? Les recherches montrent que sur la voie publique, les résultats sont disparates et dépendent de plusieurs facteurs. Par exemple, en Suisse, on constate que les infractions ont tendance à se déplacer vers les lieux où se trouve la criminalité (Kaenzig & Klauser, 2016). Ceci corrobore les analyses faites sur les personnes et sur les entreprises, à savoir que l'environnement est un élément déterminant dans l'acceptation des caméras-piétons.

Les études menées aux États-Unis, au Canada et en Suisse sur les technologies de surveillance confirment que sur la voie publique comme au sein des organisations (Diard, Lollia), le contexte a une forte influence sur les acteurs. Par exemple, les caméras-piétons des policiers semblent améliorer les rapports entre ceux-ci et les citoyens dans les zones à risques. En termes de criminalité, les effets sont plus visibles dans les pays où la population a des difficultés relationnelles avec la police que dans ceux, comme le Canada, où les rapports police/citoyens sont généralement bons. Ceci démontre que l'environnement, le lieu géographique, est un facteur déterminant dans l'impact des technologies de surveillance auprès des acteurs.

B. ...à l'acceptation des acteurs

Le modèle d'acceptation de la technologie (TAM) ne donne qu'un point de vue général sur la notion d'acceptabilité. Pour comprendre cette notion, il faut d'abord comprendre celle d'acceptation.

Selon Diard (2019), l'acceptation technologique passe par un processus d'adoption par les acteurs. Pour la vidéosurveillance, elle correspond à la capacité d'un individu à percevoir son intérêt et à donner une légitimité au système.

De nombreux chercheurs ont conduit des travaux sur les conditions d'implémentation des nouvelles technologies au sein des organisations. Il en ressort que le débat se concentre sur deux aspects : la notion d'acceptation de ces technologies par les acteurs, qui fait l'objet de nombreuses controverses, et le lien entre surveillance et protection.

Le débat sur l'implémentation des technologies de sécurité est courant dans la littérature scientifique. D'un point de vue général, l'acceptation d'une technologie correspond à l'intérêt que l'utilisateur y trouve (Suddaby & Greenwood, 2005). Que ce soit de façon groupale ou individuelle, les enjeux liés à son utilisation sont perçus et compris (Bobillier Chaumon et al.,

2006). Selon Bobillier-Chaumon et Dubois (2009), l'acceptation des technologies par le groupe ou les individus se fait grâce à un processus psychologique en trois étapes : la compréhension, l'adhésion, la légitimation du système (ou la résignation). Pour d'autres chercheurs, le processus est différent. Nous nous inscrivons, pour notre part, dans une démarche contextualisée visant une construction globale permettant l'analyse des processus émergents dans le cadre du changement (Pettigrew, 1987),(Pettigrew, 1990). Grâce à cette démarche, il est possible de comprendre l'importance des éléments externes (économique, politique, technologique et culturel) et internes (ressources humaines, processus interne) dans le contexte organisationnel. Les analyses de Kanter et Cantor montrent à quel point il est important de prendre en compte la notion de changement lorsqu'on étudie le comportement des acteurs face aux technologies et, plus spécifiquement, aux technologies de sécurité de localisation.

De nombreux chercheurs tels que Kanter introduisent à ce propos la notion de changement propre à l'acceptation d'un nouvel élément modifiant le fonctionnement d'une organisation. Selon eux, l'acceptation des nouvelles technologies par les acteurs passe par des étapes qui font partie d'un processus global. D'autres auteurs (Lollia, 2019) montrent également que pour qu'une nouvelle technologie soit plus facilement acceptée au sein d'une organisation, il est intéressant d'utiliser des méthodes d'accompagnement du changement ou des techniques telles que la « stratégie des aléas » ou la « stratégie des alliés ». Par exemple, la stratégie des alliés consiste à avoir des alliés au sein d'une organisation, lesquels faciliteront l'installation des technologies en question.

2. Les difficultés propres à l'implémentation des nouvelles technologies

L'implémentation des nouvelles technologies de sécurité au sein des organisations soulève toujours la même difficulté : la perception de l'outil de géolocalisation ou de surveillance, comme nous l'avons mentionné dans notre propos préliminaire. En effet, les acteurs le perçoivent d'un côté comme un outil de surveillance, confirmant sa pervasivité (West & Bowman, 2016), et de l'autre comme un outil de protection. Cette différence de perception peut s'expliquer par le contexte dans lequel l'outil est utilisé (culture, position des acteurs) (LOLLIA, 2019). Ainsi, il est observé que ces outils participent à la modélisation du comportement des acteurs au sein des organisations (Lollia, 2019 ; Diard, 2018).

Il faut également préciser que la notion d'acceptation de ces technologies a émergé lorsque celles-ci ont commencé à investir l'espace public. C'est parce qu'elles sont acceptées dans les rues qu'elles le sont aussi, de plus en plus, au sein des organisations, notamment dans les entreprises. On assiste ainsi à une sorte de banalisation qui alimente la pervasivité de ces technologies dans notre vie quotidienne (Claverie, 2010).

Finalement, on se rend compte que concernant les technologies de surveillance, le principal problème réside dans l'utilisation des données personnelles. Si on prend l'exemple des caméras portatives des policiers canadiens, ce qui préoccupe les citoyens n'est pas l'outil en lui-même mais plutôt le fait que leur image pourrait être diffusée sur Internet ou dans les médias (Faubert & Gendron, 2021).

La médiatisation est également un facteur d'acceptation, de la même manière que l'environnement géographique influence les acteurs.

3. Quels résultats ces technologies donnent-elles ?

Il est légitime de s'interroger sur l'effet qu'ont les caméras de surveillance sur les acteurs. Par exemple, pour les caméras-piétons des policiers, des études internationales (Adams & Mastracci, 2019)(Doiron, 2021) montrent que le fait de se sentir constamment surveillés peut engendrer du stress chez les acteurs. Certains chercheurs (Saulnier et al., 2020) évoquent même l'apparition de troubles psychologiques. Toutefois, d'autres travaux (Toronto Police Service, 2016) révèlent que les acteurs ont finalement tendance à s'y adapter et à en faire des outils pervasifs ((Claverie, 2010), c'est-à-dire intégrés à leur quotidien de façon permanente. Ils n'y prêtent quasiment plus aucune attention.

4. Solutions pour une implémentation efficace des nouvelles technologies

Nous proposons ci-dessous quelques recommandations générales pour une implémentation efficace de ces technologies, quel que soit le lieu :

- Prendre conscience de l'impact organisationnel de ce type d'outil.
- Concevoir une stratégie d'accompagnement du changement (stratégie des alliés).
- Mettre en place une stratégie de communication en amont afin d'aider les employés à accepter ces technologies, notamment en insistant sur leur aspect à la fois réglementaire et accessible (Diard) et en évitant un effet de « boîte noire », d'opacité, que l'on retrouve dans l'IA.
- Favoriser l'accès aux outils en proposant aux collaborateurs des formations permettant de les comprendre et de les maîtriser. Il est important de ne pas privilégier seulement la technicité mais d'engager également une réflexion sur l'humain et sa complexité (Lollia, 2019).
- Tenir compte de l'influence des directions, qu'elles soient politiques ou managériales.
- Construire une « culture de la sécurité ».

N'oublions pas toutefois que la vidéo protection reste aujourd'hui encore l'objet d'un combat éthique dont les résistances ne sont pas prêtes de se tasser (Boucher, 2014).

Fabrice Lollia,
Docteur en SIC
Laboratoire Dicen idf

Bibliographie

- Adams, I., & Mastracci, S. (2019). Police Body-Worn Cameras : Effects on Officers' Burnout and Perceived Organizational Support. *Police Quarterly*, 22(1), 5-30. <https://doi.org/10.1177/1098611118783987>
- Bert, J.-F. (2012). « Ce qui résiste, c'est la prison. » Surveiller et punir, de Michel Foucault. *Revue du MAUSS*, n° 40(2), 161-172.
- Bobillier Chaumon, M.-E., Dubois, M., & Retour, D. (2006). L'acceptation des nouvelles technologies d'information : Le cas des systèmes d'information en milieu bancaire. *Psychologie du Travail et des Organisations*, 12(4), 247-262. <https://doi.org/10.1016/j.pto.2006.05.002>
- Bobillier-Chaumon, M.-E., & Dubois, M. (2009). L'adoption des technologies en situation professionnelle : Quelles articulations possibles entre acceptabilité et acceptation? *Le travail humain*, 72(4), 355-382.
- Boucher, D. (2014). Les nouvelles technologies de surveillance et de contrôle : Un défi éthique. *Éthique publique*, 16(2). <https://doi.org/10.4000/ethiquepublique.1735>
- Claverie, B. (2010). *L'homme augmenté—Néotechnologies pour un dépassement du corps et de la pensée* - (L'harmattan).
- Diard, C. (2018). Psychological acceptance of organizational video surveillance. *Human Systems Management*, 37(1), 105-115. <https://doi.org/10.3233/HSM-17113>
- Diard, C. (2019). Acceptation ou refus de la vidéo-protection par les collaborateurs : Influence des facteurs de contingence lors de la mise en place de la vidéo-protection. *Recherches en Sciences de Gestion*, 1, 181-208.
- Doiron, C. (2021). *BODY-WORN CAMERAS AND ORGANIZATIONAL STRESS IN CANADIAN POLICING: A QUALITATIVE STUDY*.
- Faubert, C., & Gendron, A. (2021). Police body-worn cameras : Current state of knowledge in Canada. *Criminologie*, 54(1), 41. <https://doi.org/10.7202/1076693ar>
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British journal of sociology*, 51(4), 605-622.

- Kaenzig, R., & Klausner, F. (2016). Evaluation de la vidéoprotection dans le quartier des Pâquis. *Institut de géographie, Université de Neuchâtel.*
- LOLLIA, F. (2019). Organisation en milieu hostile : L'effet de la géolocalisation sur l'organisation en milieu terroriste. *Journal of Human Mediatized Interactions/Revue des Interactions Humaines Médiatisées, 20(2).*
- Lollia, F. (2019). *Aide à la décision en situation de crise. Les nouvelles technologies pour la prévention sécuritaire des entreprises : Limites et opportunités.* Val d'Europe. Université Paris Est Marne la Vallée.
- Pettigrew, A. M. (1987). Context And Action In The Transformation Of The Firm. *Journal of Management Studies, 24(6), 649-670.*
- Pettigrew, A. M. (1990). Longitudinal field research on change : Theory and practice. *Organization science, 1(3), 267-292.*
- Saulnier, A., Sanders, C., Lahay, R., Krupp, D., Lindsay, S., Couture-Carron, A., & Burke, K. (2020). Evaluation of the DRPS BWC Pilot Project : A report prepared for the Durham Regional Police Service. *Whitby, ON: Durham Regional Police Service.*
- Schweitzer, L. (2011). Surveillance électronique. *Communications, 88(1), 169-176.* Cairn.info.
<https://doi.org/10.3917/commu.088.0169>
- Servais, S., & Devresse, M.-S. (2019). " *Quelle est l'influence des caméras ANPR sur l'organisation du travail policier ? Surveiller plus ou surveiller mieux?*
- Suddaby, R., & Greenwood, R. (2005). Rhetorical strategies of legitimacy. *Administrative science quarterly, 50(1), 35-67.*
- Toronto Police Service. (2016). *Body-worn cameras : A report on the findings of the pilot project to test the value and feasibility of body-worn cameras for police officers in Toronto.*
- West, J. P., & Bowman, J. S. (2016). Electronic Surveillance at Work : An Ethical Analysis. *Administration & Society, 48(5), 628-651.*
<https://doi.org/10.1177/0095399714556502>