

<https://www.elcorreo.eu.org/Dossier-CONTROLE-BIOMETRIQUE-ET-VIDEOSURVEILLANCE-Contro-ler-ceux-qui-controlent>

Texte visionnaire écrit en 2016

Dossier :« Plateformes, surveillance et postpolitique dans la cybersociété »« CONTRÔLE BIOMÉTRIQUE ET VIDÉOSURVEILLANCE »

Date de mise en ligne : mercredi 20 août 2026

- Cybersociété -

Copyright © El Correo - Tous droits réservés

Le groupe d'étude sur « la cybersociété, la cybersécurité, la cyberdéfense et la protection des données à caractère personnel » du Centre d'études latino-américaines (CEL) de l'UNSAM mène une analyse comparative des tensions entre sécurité publique et libertés publiques résultant de l'expansion non réglementée des dispositifs de contrôle social en Argentine. En d'autres termes, la question est la suivante : comment les programmes de surveillance de masse affectent-ils les droits constitutionnels et la vie privée des individus lorsque l'État déserte à son rôle de contrôleur politique ?

Saga Noren, l'héroïne de la série suédoise à succès Bron Broen (Le Pont), découvre que la caméra de vidéosurveillance d'un magasin de vêtements a peut-être filmé le tueur en série qu'elle recherche. La caméra est installée à l'intérieur du magasin, dans la vitrine, et orientée vers l'extérieur.

Les enregistrements permettent en effet d'identifier une silhouette et de faire avancer l'enquête. Cependant, la police, d'une rigueur extrême, loin de remercier le propriétaire du commerce, le dénonce pour avoir installé cette caméra sans l'autorisation requise.

Auprès du public argentin, peu au fait des réglementations européennes régissant la vidéosurveillance, cette séquence fait grand bruit. On ne comprend pas tout à fait. Comment se fait-il que pour installer une simple caméra IP, de celles que l'on trouve aujourd'hui dans n'importe quelle quincaillerie, il faille obtenir une autorisation de l'État ?

Une simple promenade dans les rues de Buenos Aires révèle une ville très différente de Malmö ou de Copenhague, les deux villes où se déroule Bron Broen. Et également très différente d'autres villes européennes, en France ou en Angleterre par exemple.

La première impression est que Buenos Aires est effectivement envahie par un enchevêtrement de caméras et de câbles, disposés de manière ostensible et désordonnée non seulement à l'intérieur des commerces, des supermarchés chinois et des distributeurs automatiques, mais aussi dans l'espace public.

Il s'agit pour la plupart de caméras de vidéosurveillance de l'État, installées dans le but déclaré d'améliorer la protection des citoyens contre la menace de la criminalité. D'autres ont été installées par des particuliers à l'extérieur de leurs habitations ou de leurs commerces. Certaines agences de sécurité privées sont même allées plus loin, en installant de grands écrans VLC équipés de caméras intégrées, reliés à un centre de surveillance à distance. Sur l'écran, on voit un opérateur chargé, par roulement, de surveiller plusieurs moniteurs et plusieurs clients, et capable d'interagir en temps réel avec les personnes qui pénètrent dans les bâtiments surveillés.

Surveillance redondante

L'État national et la municipalité se sont disputé et superposé dans l'installation de « petites caméras » à Buenos Aires, suivant le modèle sécuritaire mis en avant au cours de la dernière décennie, en grande partie grâce aux stratégies de communication des caudillos de la province de Buenos Aires. C'est ce modèle de projection politique à caractère autoritaire qui « fait du bruit » dans la fiction de Malmö.

Car ce qui fait défaut dans l'imaginaire social de la sécurité publique argentine reste, en Europe, la valeur principale placée sous la protection des administrations : la vie privée et les libertés publiques. Et ce, même si les paradigmes traditionnels de la démocratie occidentale antérieurs au Patriot Act et aux attentats de Paris ont été affaiblis par le spectre du terrorisme international.

En Argentine, dix ans de campagne politico-médiatique autour du concept flou d'« insécurité » et une réponse inadéquate de la part du gouvernement national ont fini par ancrer les préjugés, renforcer la peur et, finalement, éroder l'élément central du civisme démocratique, à savoir la vie privée, à un niveau supérieur y compris à celui d'une Europe qui menace de faire resurgir l'ennemi intérieur.

La course à l'installation de systèmes de vidéosurveillance dans l'espace public a été un symptôme de l'époque, qui a accompagné la montée de la crainte des citoyens d'être victimes de la criminalité et de la violence. Ce sentiment collectif s'est d'ailleurs développé – curieusement – au rythme des progrès de la technologie numérique et de la baisse des coûts, qui a mis de nouveaux dispositifs de contrôle, de surveillance et d'espionnage à la portée des États et même des simples citoyens.

Parallèlement, le gouvernement mis en place en 2003 s'était fixé pour objectif de passer de stratégies policières coercitives à une stratégie fondée sur la prévention et, en matière d'ordre public, sur la persuasion comme forme de négociation permanente et d'application souple de la loi.

Dans ce processus d'« euphémisation des stratégies policières » [1], l'évolution technique des équipements et des tactiques a joué un rôle important. La réponse de la « sécurité démocratique » aux revendications sociales contre l'insécurité a consisté en une combinaison des meilleures intentions afin de ne pas stigmatiser les populations défavorisées et à miser sur la modernisation technologique pour gagner la confiance des citoyens dans la gestion de la sécurité publique par le gouvernement.

L'extension de ces nouveaux développements dans les communes de la banlieue, grâce à un financement national, a alors constitué un élan significatif.

C'est pourtant ce qui a marqué le coup d'envoi de l'engouement des dispositifs de contrôle technique des personnes. Ce sont les maires qui ont franchi le pas en se précipitant pour acheter (ou louer) des caméras, un peu comme des pompiers s'empressant d'éteindre l'incendie de l'insécurité, sans se renseigner sur leur efficacité réelle en matière de prévention de la criminalité, sans chercher à accompagner ces installations par des mécanismes d'évaluation systématique de leur efficacité, et sans se soucier des effets que pourrait avoir cette intrusion dans la vie privée des personnes [2].

Le gouvernement national et populaire est tombé dans le piège de la prétendue neutralité de ces gadgets et – par naïveté ou en suivant l'élan des fournisseurs de ces technologies – est entré sur le champ de bataille avec les armes et les idées de ses adversaires. Dans le cadre d'un marchandage sans scrupules avec les entreprises médiatiques, le gouvernement est allé jusqu'à autoriser C5N à installer ses propres caméras vidéo dans l'espace public, en échange de quoi cette chaîne d'information mettait ses signaux à la disposition du centre d'opérations de la Police fédérale argentine.

Quoi qu'il en soit, face à l'indifférence des citoyens quant à l'atteinte à la vie privée, la gauche et la droite se sont disputé le rôle de fer de lance en matière de contrôle social de la population.

Les uns ont utilisé ces nouveaux dispositifs comme une mise en scène de leur stratégie politico-communicationnelle, tandis que les autres l'ont fait, convaincus que toute modernisation permettrait de répondre aux nouvelles formes de

criminalité et de violence, tout en facilitant le contrôle politique des forces de police.

Dans tous les cas, il en résulte un héritage qui pèse, tant sur le plan idéologique que structurel, sur les fondements mêmes d'une société qui se revendique démocratique, et qui élargit le champ d'ingérence des appareils de coercition étatiques dans la vie quotidienne, au point d'éroder les frontières entre la sphère publique et la sphère privée.

Telle avait été la mise en garde très tôt du lanceur d'alerte Julian Assange, fondateur du site *Wikileaks*. En juin 2013, Assange a déclaré au site d'information Infobae que « [l'Argentine dispose du système de surveillance le plus agressif d'Amérique](#) ».

L'analyste ne faisait pas référence à cette prolifération de caméras. Il évoquait le SIBIOS, le Système fédéral d'identification biométrique pour la sécurité, créé par le gouvernement de Cristina Fernández [3]. Ses déclarations, formulées depuis l'ambassade de l'Équateur à Londres, où il est toujours réfugié depuis plus de cinq ans (texte écrit en 2016), sont restées sans écho. Le SIBIOS était peu connu en Argentine, non pas par manque d'engagement de la part des autorités, mais plutôt en raison du black-out médiatique qui rendait invisible toute action gouvernementale pouvant sembler proactive en matière de lutte contre la criminalité et la violence.

Mais qu'est-ce que le SIBIOS ?

Ce système est-il toujours en place ou a-t-il déjà été démantelé par les nouvelles autorités, dans la lignée de la contre-révolution accélérée menée par le gouvernement Macri ?

Le SIBIOS était-il la chimère panoptique dénoncée par Assange ?

Qui gère ce système et celui de la vidéosurveillance d'État qui centralise les informations sensibles sur les personnes, alors que la Police fédérale argentine est en pleine désorganisation ?

Quels sont les mécanismes de contrôle étatique, parlementaire, citoyen ou judiciaire de ce système ?

Quel est l'organe chargé de veiller à la protection des données personnelles, au droit à l'image et de faire face à l'intrusion incontrôlée des services de police dans la vie privée des citoyens ?

Où en est l'analyse de la tension entre la nécessité d'optimiser la réponse de l'État face aux défis actuels de la criminalité et la protection des libertés qui garantissent la qualité de la démocratie ?

Répondre à ces questions dans une perspective géopolitique et en dialogue avec des équipes universitaires françaises et suédoises constitue l'axe central du projet lancé par le groupe d'études sur la cyber-société, la cybersécurité, la cyberdéfense et la protection des données à caractère personnel (C3PDP) du Centre d'études latino-américaines (CEL) de l'Université Nationale de San Martín.

Pour répondre à certaines de ces questions, il faudra tout d'abord exposer l'objet de cette étude, qui consiste en réalité en un ensemble de solutions technologiques, de normes, de réglementations, de lois et de jurisprudence ; il faudra également anticiper certaines conclusions concernant les modes d'organisation de la société dans leur rapport avec la sécurité publique, la protection des libertés civiles et la vie privée.

Afin d'évaluer l'actualité de ces systèmes de surveillance et le rôle de l'État (ou son désengagement) dans la réglementation du développement des réseaux privés de vidéosurveillance et de contrôle biométrique de la population, il faudra analyser la logique qui sous-tend les décisions du nouveau gouvernement, la force ou la fragilité institutionnelle de ses organes de contrôle (le cas échéant), en tenant compte des facteurs qui relient le changement politique à la structure bureaucratique et administrative actuelle, ainsi que des capacités effectives du gouvernement à relever les défis liés à la gestion de cet appareil, de ses effets sur la stabilité du gouvernement politique et de son impact sur la qualité de la démocratie elle-même.

Des caméras, des caméras et encore des caméras

Le SIBIOS dénoncé par Assange, par exemple, fait partie d'un ensemble d'innovations technologiques menées principalement dans la capitale fédérale, mais ayant une portée nationale, mises en œuvre pendant une brève période après la création du ministère de la Sécurité nationale, en décembre 2010.

Une partie de cet écosystème est ce que le gouvernement précédent appelait « Buenos Aires Ciudad Segura » [4], un réseau de vidéosurveillance, de gestion des alertes policières et de répartition opérationnelle des ressources (agents, voitures de patrouille, camions de pompiers) via le numéro de téléphone 911, confié à la société israélienne MER [5].

Un sous-système intègre également le réseau de vidéosurveillance sur les quais des trains urbains (dont la surveillance est assurée par la Direction de la police ferroviaire), un autre sous-système sert à soutenir les enquêtes judiciaires dans les affaires impliquant des armes à feu (Système d'information balistique, SAIB) et un autre encore est dédié à l'identification biométrique des visages dans le cadre d'enquêtes judiciaires [6].

Les systèmes de vidéosurveillance, de commandement et de contrôle, d'une part, et d'identification biométrique, d'autre part, présentent des points de convergence qui devront être pris en compte dans le cadre d'une enquête sur les effets de ces dispositifs en lien avec les libertés publiques. En principe, ces deux systèmes sont gérés par la Police fédérale argentine, organisme qui connaît actuellement une transformation profonde depuis l'arrivée au pouvoir de Mauricio Macri.

Ces deux systèmes sont mis en œuvre sur des plateformes informatiques gérées techniquement par un seul service de cet organisme policier aujourd'hui scindé, la Superintendance des communications, avec une intervention discrète du ministère de la Sécurité en matière de contrôle (qui dépend en réalité davantage de la volonté politique et personnelle des fonctionnaires que de mécanismes institutionnels).

La centralisation des bases de données, *des datas centers*, des centres de surveillance et de la gestion des réseaux au sein d'un seul service d'un organisme public spécialisé dans la coercition légale fait partie des défis auxquels est confrontée l'Argentine moderne : un modèle de sécurité conçu sans tenir compte des précautions requises par ces questions sensibles.

Ce « nouveau » système, mis en place entre 2011 et 2013, est resté inchangé jusqu'à aujourd'hui, malgré certains dysfonctionnements survenus avec les fournisseurs israéliens de la technologie du système 911, l'ancien Comando Radioléctrico désormais connu sous le nom de Centre de commandement et de contrôle [7].

Cependant, certains signes à l'horizon sont source d'inquiétude. Le gouvernement précédent avait mis au point un sous-système de vérification géoréférencée 24 heures sur 24 et 7 jours sur 7 des effectifs de police en intervention. Les patrouilleurs et les agents étaient surveillés en temps réel par le secrétaire à la Sécurité nationale, un contrôle à la fois personnel et institutionnel. Ce contrôle minimal mis en place a été désactivé par les nouvelles autorités, suivant une ligne politico-idéologique d'autonomisation des forces de police.

La surveillance de masse exercée par l'État est intrinsèquement répressive, même si les autorités ne prennent pas de mesures physiques à l'encontre des personnes, telles que la manipulation d'informations privées ou des arrestations. L'abandon du contrôle politique constitue un écart par rapport aux objectifs que doit poursuivre une institution d'autorité dans une république, à savoir se soumettre à des mécanismes institutionnels de contrôle.

L'absence d'évaluations qualitatives et quantitatives des mesures mises en œuvre tant par ce gouvernement que par celui qui l'a précédé est révélatrice de cette situation. En partant d'une approche des problèmes fondée sur le bon sens, on est parvenu à un phénomène inverse de celui proclamé : à force d'éteindre des incendies, on colmate des brèches ici et là de manière pragmatique, sans contrôles ni évaluations des politiques publiques. En l'absence de contre-pouvoirs républicains, la force coercitive impose des limites aux libertés et risque de façonner des individus aliénés en les amenant à intérioriser leurs surveillants. Elle impose des mécanismes de contrôle immatériels, aux effets plus durables et permanents. La surveillance globale, y compris celle du cyberspace (de plus en plus hybridée avec l'espace physique et matériel), normalise les schémas d'autocensure.

Quel est le système d'hégémonie qui se maintient lorsque la surveillance se dissocie du gouvernement politique ?

L'autonomisation des organes répressifs de l'État chargés de veiller à la sécurité de ses citoyens et à la défense de ses intérêts vitaux est au cœur de ces fonctions républicaines et impose un nouvel ordre du jour, renforcé et mondialisé par les technologies de contrôle et d'information.

Pour revenir à l'exemple initial, il convient de souligner que la vidéosurveillance peut être (et doit être) un élément de la lutte contre la criminalité et la violence. Ces dispositifs peuvent et doivent également contribuer à la gestion de l'espace public, faciliter la circulation, contribuer à la santé publique, ainsi qu'à l'entretien des infrastructures des zones sous surveillance. Ils ont un effet dissuasif et renforcent également le sentiment de sécurité. Déployés de manière rationnelle, dans le cadre d'une stratégie systématique de renseignement criminel et avec la participation des citoyens, ils constituent les mécanismes d'une tactique de prévention « situationnelle ».

Cependant, contrairement à d'autres démocraties occidentales, en Argentine, ces dispositifs ont été mis en place et continuent de se développer sans doctrine d'utilisation, sans contrôle parlementaire, sans critères de révision, sans supervision d'une autorité étatique, urbanistique, judiciaire, nationale, provinciale ou municipale chargée de protéger le droit à la vie privée des citoyens [8].

La surveillance des entreprises et celle de l'État ne suivent pas des voies distinctes. Elles développent plutôt des alliances d'intérêts, en particulier dans le domaine d'Internet. De nombreuses informations obtenues par le biais des systèmes de surveillance circulent entre le secteur public et le secteur privé, dans les deux sens.

Le programme C3PDP du CEL se propose donc de décrypter les tensions qui surgissent lors de changements gouvernementaux disruptifs, tels que celui que traverse actuellement l'Argentine ou ceux qui pourraient survenir en Europe avec la montée des populismes de droite. Une perspective comparative peut permettre de tirer des enseignements importants sur les doctrines d'intervention, les savoirs professionnels et les pratiques courantes des agences de sécurité publiques et privées.

En d'autres termes, nous nous proposons d'étudier les évolutions de la gestion de la sécurité publique à la croisée entre la fragilisation des appareils de contrôle politique, et l'indifférence parlementaire et citoyenne, et enfin l'efficacité des dispositifs bureaucratiques et coercitifs mis en place.

SIBIOS et la protection des données personnelles

La mise en place du SIBIOS, géré sous l'égide de la Direction générale de la police scientifique (1er étage, 670 Azopardo), avait pour objectif de permettre aux forces de l'ordre nationales de disposer d'informations permettant d'identifier tous les citoyens grâce à un logiciel de dernière génération. Cet idéal de contrôle sans distinction de «

tous les individus », qu'ils soient ou non impliqués dans des affaires judiciaires, s'est concrétisé grâce à un accord interjuridictionnel avec le Registre national des personnes [9]. Le système ainsi mis en place, qui s'appuie sur le logiciel du Système automatisé d'empreintes digitales (AFIS), traite les données nominatives et biologiques, à savoir les empreintes digitales et les photographies, afin d'assurer une identification efficace des personnes et des indices.

L'objectif était ainsi d'optimiser les enquêtes scientifiques sur les délits et de renforcer la fonction préventive en matière de sécurité. Le ministère de la Sécurité fera office d'autorité chargée de la mise en œuvre de ce nouveau système, qui sera utilisé par la police fédérale, la gendarmerie nationale, la préfecture navale, la police de sécurité aéroportuaire, le Registre national des personnes et la Direction nationale des migrations. De plus, le dispositif est conçu pour intégrer les provinces au système. En d'autres termes, les concepteurs du système étaient convaincus que le renforcement institutionnel du ministère de la Sécurité, en tant que chef de file du système, servirait en soi de contrepoids au pouvoir de la police et de garant des libertés publiques et de la vie privée, qui pourraient être affectées.

Dans le même temps, il était nécessaire de modifier le modèle de gestion de la sécurité publique pour adopter un modèle fondé sur la capacité technique à gérer des informations à grande échelle. Il s'agissait en d'autres termes de professionnaliser les systèmes de renseignement criminel afin d'améliorer la contribution de la police à la justice.

Bien que le système automatisé AFIS fût déjà partiellement utilisé au sein de la Police fédérale argentine depuis une décennie, l'innovation a consisté à intégrer automatiquement ses bases de données aux informations d'identité, aux empreintes digitales et aux photographies des personnes qui renouvellent leurs documents (passeports et cartes d'identité) ou qui demandent une nouvelle carte d'identité auprès du RENAPER.

Ainsi, un corps de police – et plus encore un seul service de la PFA – intègre toutes les données relatives à des personnes innocentes, dans l'hypothèse où celles-ci pourraient éventuellement commettre des délits ou être impliquées dans des procédures judiciaires.

[Diego Llumá*](#) pour [Cuadernos del CEL](#)

[Cuadernos del CEL](#). 2016, vol. I, n° 2. p. 6-15. ISSN : 2469-150X

***Diego Llumá** est enseignant et chercheur universitaire. Ex-Directeur National de Coopération Régionale et Internationale du Ministère de la Sécurité de la Nation. Il enseigne la « Coopération internationale » à l'Université Métropolitaine pour l'Éducation et le Travail et la « Géopolitique des réseaux et le capitalisme de surveillance » à l'Université Nationale de Saint Martin en Argentine. Diplômé en Sciences de la Communication Sociale (UBA). Il a suivi des masters sur la Défense Nationale et la Stratégie (l'Université Nationale de La Plata - centre d'Études pour la Nouvelle Majorité) ; de l'Institut de Hautes Études de l'Amérique Latine (l'Université de Paris III, de Sorbonne Nouvelle, France), de l'Institut Français de Géopolitique (l'Université de Paris VIII, de Seine-Saint Denis, France). Il est *Visiting Fellow* du *Bulletin of the Atomic Scientists* (Chicago, USA) et de la [Fondation Journalistes de Europe](#) (Paris, France).

Traduit de l'espagnol depuis [El Correo de la Diáspora](#) par : Estelle et Carlos Debiasi.

[El Correo de la Diaspora](#). Paris, le 26 août 2026.

[1] FILLIEULE, Olivier-Donatella DELLA PORTA (dir.), Police et manifestants. Maintien de l'ordre et gestion des conflits, Paris, Les Presses

Sciences Po, 2006.

[2] Qui comprennent également la mise en place de centres de surveillance, souvent qualifiés de manière pompeuse de « commandement et contrôle ».

[3] Le Système fédéral d'identification biométrique pour la sécurité « SIBIOS » a été créé à la suite de la promulgation du décret n° 1766/2011 et comprend un ensemble de sous-systèmes biométriques, centralisés, organisés et interconnectés, qui visent à permettre l'identification rapide des personnes.

[4] « Le projet « Buenos Aires Ciudad Segura » s'inscrit dans le cadre des objectifs du ministère de la Sécurité visant à moderniser les forces de sécurité, et en particulier, à ce stade, la police fédérale, grâce à l'intégration d'outils technologiques de dernière génération destinés à la prévention et à la lutte contre la criminalité », indiquait l'un des rapports ministériels communiqués à la presse en 2013.

[5] Cf. <http://www.mer-group.com/es>

[6] Le système AFIS MetaMorpho est une solution évolutive à la pointe de la technologie, capable d'offrir des services externes tels que la connexion de stations distantes, la consultation, la recherche et la saisie. Ce système est évolutif, ce qui permet d'augmenter la capacité de la base de données.

[7] Informations institutionnelles sur le projet « Buenos Aires Ciudad Segura » sur le site web de la société MER.

<http://www.mer-group.com/wp-content/uploads/2013/10/Buenos-Aires-Case-Study-En.pdf>

[8] « Le secret consiste à conférer des pouvoirs aux forces de police sans leur donner la possibilité d'en abuser. Nous avons autant besoin de la sécurité que nous procure le gouvernement que d'être protégés contre ce dernier », souligne le cryptographe Bruce Schneier dans « *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World* », W. W. Norton & Company, 2016.

[9] Le Registre national des personnes, organisme décentralisé du ministère de l'Intérieur, est chargé de l'enregistrement et de l'identification des personnes physiques domiciliées sur le territoire argentin ou relevant de la juridiction argentine, ainsi que de la délivrance de la carte d'identité nationale et des passeports nationaux.