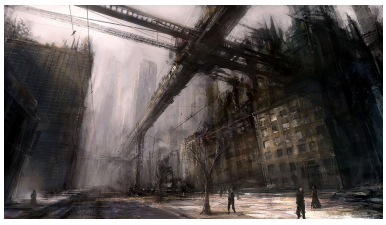
https://www.ricochets.cc/Chronique-de-la-technopolice-8-ans-de-videosurveillance-biometrique-illegale-drones-partout-reconnaissance-faciale-generalisee-surveillance-algorithme-allocataires-CAF-et-CNIL-complice-fichage-illegal-police-municipale.html

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF et la CNIL complice, fichages

illégaux par les polices municipales...

- Les Articles -



Date de mise en ligne : jeudi 14 mars 2024

Les brutalités policières structurelles sont maintenant bien connues, même si l'impunité règne et que les médias dominants ne les évoquent guère.
En revanche, la technopolice, le fichage généralisé, la surveillance logicielle automatisée...passent souvent sous les radars et se déroulent sans entraves.
Plus insidieuse et invisible que les yeux crevés au LBD, les cranes explosés, les tués par les flics et les mains arrachées par leurs grenades, la technopolice est pourtant également un terrible poison et une incarcération quotidienne dans les filets mortels de l'Etat et du Capital.

La surveillance et la coercition généralisées ne concernent pas seulement les agissements des milices armées policières radicalisées, les « gentilles » administrations dites sociales et leurs fonctionnaires embarqués de gré ou de force sont également en première ligne de la surveillance totale et du contrôle, légal ou illégal, en mode Big Brother. Des employés font Â« leur travail Â» efficacement, tout comme les anciens agents zélés du nazisme ou les agents des pires entreprises capitalistes.
Tous ont besoin d'emplois n'importe lequel, et l'exécutent ; cette injonction permanente au travail pour avoir une valeur sociale et de l'argent est une des pires saloperies piégeuses de l'Etat-capitalisme. Avec la perte croissante des moyens de subsistance et l'accroissement de la précarité, cette pression mortifère s'accentue et étouffe tout le monde à la gorge, pire qu'un anaconda.

On veut respirer !

On veut respirer ! pas s'étouffer avec les remugles moisis de la froide gestion numérique totalitaire étatico-capitaliste.
Si la technopolice et les rationalités cybernétiques (IA) semblent indispensables à l'Etat-capitalisme, l'Etat-capitalisme n'est pas indispensable à l'existence de sociétés humaines.

- Voici quelques terribles et édifiantes illustrations de la nocivité de la technopolice :

Notation des allocataires : la CAF étend sa surveillance à l'analyse des revenus en temps réel

- **Notation des allocataires : la** CAF étend sa surveillance à l'analyse des revenus en temps réel

Retrouvez l'ensemble de nos publications, documentations et prises de positions sur l'utilisation par les organismes sociaux - CAF, Pôle Emploi, Assurance Maladie, Assurance Vieillesse - d'algorithmes à des fins de contrôle social sur notre page dédiée et notre gitlab.

Il y a tout juste deux mois, nous publiions le code source de l'algorithme de notation des allocataires de la CAF. Cette publication démontrait l'aspect dystopique d'un système de surveillance allouant des scores de suspicion à plus de 12 millions de personnes, sur la base desquels la CAF organise délibérement la discrimination et le sur-contrôle des plus précaires. Ce faisant, nous espérions que, face à la montée de la contestation, les dirigeant·es de la CAF accepteraient de mettre fin à ces pratiques iniques. Il n'en fut rien.

À la remise en question, les responsables de la CAF ont préféré la fuite en avant. La première étape fut un contre-feu médiatique où son directeur, Nicolas Grivel, est allé jusqu'à déclarer publiquement que la CAF n'avait ni « à rougir » ni à s'« excuser » de telles pratiques. La deuxième étape, dont nous venons de prendre connaissance, est bien plus inquiétante. Car parallèlement à ses déclarations, ce dernier cherchait à obtenir l'autorisation de

démultiplier les capacités de surveillance de l'algorithme via l'intégration du suivi en « temps réel » des revenus de l'ensemble des allocataires. Autorisation qu'il a obtenue, avec la bénédiction de la CNIL, le 29 janvier dernier.
(...)
Désormais, l'algorithme de la CAF bénéficiera d'un accès en « temps réel » aux ressources financières de l'ensemble des 12 millions d'allocataires (salaires et prestations sociales).
(...)
La justification d'une telle extension de la surveillance à l'oeuvre à des fins de notation des allocataires est d'accroître la « productivité du dispositif [de l'algorithme] » selon les propres termes des responsables de la CAF8. Qu'importe que se multiplient les témoignages révélant les violences subies par les plus précaires lors des contrôles9. Qu'importe aussi que les montants récupérés par l'algorithme soient dérisoires au regard du volume des prestations sociales versées par l'institution.
(...)

La CNIL devient une simple agence de com au service du fichage administratif intégral de la population

Nulle part n'apparaît la moindre critique politique d'un tel dispositif, alors même que cela fait plus d'un an que, aux côtés de différents collectifs et de la Défenseure des Droits, nous alertons sur les conséquences humaines désastreuses de cet algorithme. La CNIL alerte par contre la CNAF sur le risque médiatique auquelle elle s'expose en rappelant qu'un scandale autour d'un algorithme en tout point similaire a « conduit le gouvernement néerlandais à démissionner en janvier 2021 ». Une illustration caricaturale de la transformation du « gendarme des données » en simple agence de communication pour administrations désireuses de ficher la population.
(...)
Le ciblage des plus précaires par l'algorithme de la CAF n'est donc pas accidentel mais nécessaire à l'atteinte de son objectif politique : assurer le « rendement des contrôles ». La seule façon d'éviter de tels « biais » est donc de s'opposer à l'usage même de l'algorithme.
(...)

Un risque majeur en termes de surveillance et de protection de la vie privée

cette automatisation nécessite en retour que soit déployée **la plus grande infrastructure numérique jamais créée à des fins de récolte, de partage et de centralisation des données personnelles de la population française (impôts, CAF, Assurance-Maladie, Pôle Emploi, CNAV, Mutualités Sociales Agricoles....)**. De par sa taille et sa nature, cette infrastructure pose un risque majeur en termes de surveillance et de protection de la vie privée.
(...)

Voir aussi : **Dystopie au quotidien : la** CAF et d'autres administrations traquent les plus précaires à coup d'algorithmes discriminatoires - Surveillance numérique généralisée et automatisée, comme en Chine ?

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

L'activisme écologiste, nouveau terrain d'expérimentation de la Technopolice

L'activisme écologiste, nouveau terrain d'expérimentation de la Technopolice

Plusieurs affaires récentes ont mis en lumière la surveillance particulièrement intensive subie par les militantes écologistes. Outre l'arsenal administratif et répressif déployé par l'État pour les punir, c'est la nature des moyens utilisés qui interpelle : drones, reconnaissance faciale, marqueurs codés... Le ministère de l'Intérieur expérimente et perfectionne sur les activistes écologiques ses outils technopoliciers.

Plusieurs articles ont révélé le caractère intensif des moyens de surveillance et de répression déployés par l'État pour punir certaines actions militantes écologistes. Si cela avait déjà été documenté pour le mouvement de résistance nucléaire à Bure, c'est dernièrement le cas de l'affaire Lafarge pour laquelle un article paru sur Rebellyon a détaillé les outils mis en oeuvre par la police afin d'identifier les personnes ayant participé à une action ciblant une usine du cimentier.

Vidéosurveillance, analyse des données téléphoniques, réquisitions aux réseaux sociaux, relevés ADN, virements bancaires, traceurs GPS... La liste paraît infinie. Elle donne une idée de la puissance que peut déployer l'État à des fins de surveillance, « dans un dossier visant avant tout des militants politiques » - comme le souligne Médiapart dans son article.

Pour avoir une idée de l'étendue complète de ces moyens, il faut y ajouter la création des cellules spécialisées du ministère de l'Intérieur (la cellule Démeter, créée en 2019 pour lutter contre « la délinquance dans le monde agricole » et la cellule « anti-ZAD », mise en place en 2023 à la suite de Sainte-Soline) ainsi que l'alerte donnée par la CNCTR (l'autorité de contrôle des services de renseignement) qui en 2023 a souligné son malaise sur l'utilisation accrue des services de renseignement à des fins de surveillance des organisations écologistes.

Les forces de sécurité semblent continuer de perfectionner et expérimenter sur les organisations écologistes leurs nouveaux outils de surveillance : drones, caméras nomades, reconnaissance faciale, produits de marquages codés... Parce que ces organisations leur opposent une résistance nouvelle, souvent massive, déployée sur un ensemble de terrains différents (manifestations en milieu urbain, ZAD, méga-bassines...), les forces de police semblent trouver nécessaire l'utilisation de ces outils de surveillance particulièrement invasifs.
(...)

La France est à l'avant-garde de la dérive autoritaire en Europe

Les mouvements militants ne sont évidemment pas les seuls à connaître cette intensité dans le déploiement des moyens de surveillance : les exilées, les habitantes des quartiers populaires ont toujours été les premières à subir la militarisation forcenée des forces du ministère de l'Intérieur. **Néanmoins, cette expérimentation des technologies sur les organisations écologistes est une nouvelle preuve de l'escalade sécuritaire et déshumanisée de la police et de la gendarmerie en lien avec la criminalisation des mouvements sociaux. La France est à l'avant-garde de la dérive autoritaire en Europe, puisqu'il semble être l'un des pays du continent ayant une pratique régulière et combinée de ces nouveaux outils**

Vidéosurveillance algorithmique à la police nationale : des révélations passibles du droit pénal

Vidéosurveillance algorithmique à la police nationale : des révélations passibles du droit pénal - Dans un article publié aujourd'hui, le média d'investigation Disclose révèle que depuis des années, en se sachant dans l'illégalité la plus totale, la police nationale a recouru au logiciel de l'entreprise israélienne Briefcam, qui permet d'automatiser l'analyse des images de vidéosurveillance. Cette solution comporte une option « reconnaissance faciale » qui serait, d'après Disclose, « activement utilisée ».
(...)

La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale

en raison des dissimulations dont ce marché public hautement sensible a fait l'objet de la part de hauts fonctionnaires et de responsables politiques.
(...)
Tout aussi choquant est le sentiment d'impunité généralisé que révèle cette affaire. Les cadres de la Direction Générale de la Police Nationale, de même que les ministres successifs, ont sciemment organisé le secret par peur de la controverse, se sachant hors du droit.
Rappelons-le : « Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. » (cf. art. 226-18 et -19 du code pénal). Par ailleurs, tout·e fonctionnaire est tenu·e de signaler sur le champ une infraction dont il ou elle aurait connaissance au procureur (article 40 du code de procédure pénale). Enfin, Disclose explique que pour financer le renouvellement des licences Briefcam, « la hiérarchie policière a pioché dans le « fonds concours drogue » ». Ce qui pourrait s'apparenter à du détournement de fonds publics.
(...)
Ces faits sont extrêmement graves. L'impuissance chronique à laquelle se condamnent les contre-pouvoirs institutionnels, de la CNIL à l'IGPN, est elle aussi symptomatique d'une crise systémique de l'État de droit
(...)

Depuis huit ans, le ministère de l'intérieur dissimule le recours à cet outil qui permet l'emploi de la reconnaissance

faciale

Sur Disclose : **La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale**

En 2015, les forces de l'ordre ont acquis, en secret, un logiciel d'analyse d'images de vidéosurveillance de la société israélienne Briefcam. Depuis huit ans, le ministère de l'intérieur dissimule le recours à cet outil qui permet l'emploi de la reconnaissance faciale.

(...)

D'après des documents internes au ministère de l'intérieur obtenus par Disclose, **les forces de l'ordre utilisent les systèmes de Briefcam depuis 2015, dans le plus grand secret. Le logiciel en question, baptisé « Vidéo Synopsis », permet de traquer une personne sur un réseau de caméras grâce, par exemple, à la couleur de son pull. Il peut également suivre un véhicule à l'aide de sa plaque d'immatriculation ou examiner plusieurs heures de vidéos en quelques minutes.** Le slogan de Briefcam, rachetée par le géant de la photo Canon en 2018 : « Transformer la vidéosurveillance en intelligence active ».

(...)

Cette possibilité offerte par Briefcam a d'ailleurs été mise en avant comme un véritable « plus » par le service en charge des outils technologiques au sein de la DGPN. Dans un courriel envoyé en novembre 2022, un haut-gradé de la police explique que le logiciel possède des « fonctionnalités comme : les plaques d'immatriculation, les visages », mais aussi « des fonctionnalités plus « sensibles » » telles que la « distinction de genre, âge, adulte ou enfant, taille ». Il précise enfin que certains modules de l'application permettent de « détecter et d'extraire des personnes et objets d'intérêts a posteriori », mais aussi de faire de l'analyse vidéo en « temps réel ».

(...)

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

VERS LA GÉNÉRALISATION DES DRONES

- **Le Conseil Constitutionnel s'y était opposé en 2021, le gouvernement vient d'officialiser l'usage des drones policiers**

Le décret sur l'utilisation des drones équipés de caméras, notamment pour le maintien de l'ordre et la surveillance

des frontières, a été publié jeudi 20 avril au Journal Officiel.

Généralisation de l'usage des drones par la police

Le texte autorise l'utilisation de drones par les policiers, gendarmes, douaniers ou militaires, dans un grand nombre de cas et avec des termes assez flous : pour « la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés », pour « la sécurité des rassemblements » sur la voie publique, ainsi qu'en « appui » des agents « au sol » « en vue de leur permettre de maintenir ou de rétablir l'ordre public ». Bref, c'est la généralisation de l'usage des drones par la police.

Pour rappel, ce déploiement s'est fait en plusieurs étapes. En pleine crise sanitaire, le 27 mars 2020, le gouvernement avait lancé une grande commande d'environ 200 drones pour un déploiement rapide sur le territoire. En parallèle, des préfets comme Didier Lallement à Paris avaient utilisé des drones de surveillance en-dehors du cadre légal contre des manifestations.

Ce cadre légal avait été prévu par la loi « sécurité globale » fin 2020. La fameuse loi de Darmanin, qui prévoyait d'interdire de filmer les policiers et qui avait mis des centaines de milliers de personnes dans la rue. Le Conseil Constitutionnel avait retoqué l'autorisation des drones dans cette loi. Le Conseil d'État et la CNIL avaient aussi condamné l'usage de drones.

Mais ce revers n'avait pas arrêté le gouvernement, preuve qu'il se moque bien du Conseil Constitutionnel lorsqu'il ne va pas dans son sens. Un an plus tard, en décembre 2022, les macronistes faisaient passer la « loi sur la responsabilité pénale et la sécurité intérieure », une énième batterie de mesures sécuritaire. L'occasion de faire passer les mesures refusées par le Conseil Constitutionnel l'année précédente. **Cette fois c'est la bonne. Après 3 revers, le décret sur les drones est passé.**

Ce déploiement s'accompagne de mesures sur la reconnaissance faciale. Dans une indifférence générale, un « projet de loi JO 2024 » a été déposé en tout discrétion, pendant les fêtes de fin d'année 2022. **Il prévoit une vidéosurveillance de masse appuyée par l'Intelligence Artificielle. L'article 7 autorise « à titre expérimental » l'utilisation en temps réel de systèmes d'intelligence artificielle pour analyser les images des drones et des caméras de surveillance. Une première en France et en Europe.**

L'acharnement du gouvernement paie. Les flics pourront désormais les utiliser à loisir dans l'espace public, et les prochaines mobilisations seront sous un ciel occupé. Quadrillé par ces oiseaux robotisés au service de l'ordre policier.

Cette surveillance n'est pas imbattable. Lors des Gilets Jaunes, les flics chargés de télépiloter des drones « ont dû procéder à quelques replis stratégiques et atterrissages d'urgence pour échapper à la vindicte des goélands ». D'autres attaques ont été organisées par les corneilles, notamment durant les manifestations. Des aigles ont aussi mis hors-service des drones en montagne.

En novembre 2021au Burkina Faso, un adolescent équipé d'un lance-pierre traditionnel avait abattu un drone français qui surveillait un rassemblement visant à empêcher le passage d'un convoi de l'armée française.

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

LES PRODUITS DE MARQUAGE CODÉS (PMC) : LA SUBSTANCE POUR CRIMINALISER ET TRACER LES MANIFESTANT-ES

Dans la gamme de l'arsenal qui porte atteinte à la liberté de manifester on trouve les PMC, pour « produits marqueurs codés », encore hors de toute législation et pourtant utilisés par les forces répressives depuis les Gilets Jaunes.

Il s'agit d'un produit chimique projeté, soit en spray, soit sous forme de bille avec un fusil à air comprimé type EMF 100 (un genre de flingue de paintball, équipé d'un télémètre avec une portée de précision de 30 à 40 mètres), sur les manifestant-es en vue de les tracer pour faciliter ensuite les interpellations. À l'instar du bétail ou des bagnards, les militant-es sont aussi marqués. Sur les photos de cette arme prises à Sainte-Soline, on identifie le réservoir de billes ainsi qu'un viseur holographique Eotech très précis, qui équipe aussi les LBD, attaché sur le canon de l'arme. Le tireur porte une caméra sur son casque, il est donc probable que l'identification avec les PMC fonctionne à l'aide d'images accompagnant le tir, pour caractériser les faits reprochés aux personnes ciblées. « L'unicité des codes confère à la technologie un caractère particulièrement discriminant » pour faire condamner une personne, estime la gendarmerie.

Il existe deux types de marqueurs :

- les marqueurs colorés, qui permettent une identification visuelle directe et de tous,
- les marqueurs de type « ADN », composés d'ADN de synthèse, qui sont inodores, incolores, persistants plusieurs semaines sur les vêtements ou sur la peau et qui se révèlent aux ultra-violets. Les flics préconisent alors de fermer les yeux car les rayons peuvent potentiellement être dangereux, merci de prendre soin de notre santé !

À Sainte-Soline le 25 mars, deux personnes au moins ont été placées en garde-à-vue sur le fondement de la détection (à l'aide de lampes UV) de PMC sur leurs vêtements et leur peau.

Le bug, c'est qu'avec la lampe UV, d'autres traces d'ADN peuvent apparaître, la vôtre si vous avez bavé en mangeant trop goulûment, celle de votre voisin sympathique qui a tendance aux postillons... S'en suivra alors une deuxième expertise impliquant l'IRCGN (Institut Recherche Criminelle de la Gendarmerie Nationale) qui fera un prélèvement de la trace pour analyse. Si l'ADN concorde, banco, vous serez bon pour la garde à vue au motif d'avoir « participé sciemment à un groupement, même formé de façon temporaire, en vue de la préparation, caractérisée par un ou plusieurs faits matériels, de violences volontaires contre les personnes ou de destructions ou dégradations de biens » (CF Art 222-14-2 du code pénal, puni d'un an d'emprisonnement et de 15 000 Euros d'amende). Un crime d'intention, basé sur aucun fait concret...

Les flics pourront également, lors de cette nouvelle expertise, demander un prélèvement de votre ADN, mais vous pouvez en toute légalité refuser si vous êtes dans le cadre d'une enquête préliminaire. Ne cédez pas à cette pression, pour que le refus d'ADN soit considéré comme un délit il faut une preuve d'infraction (CPP Art 706-55). Le maître mot reste que vous n'avez « rien à déclarer ».

Que vous ayez été visé intentionnellement, ou par « inadvertance » suite à un tir de « haute précision », ou encore par contact avec un tiers qui a reçu le produit (qui met 5 minutes à sécher), cela pourra être un motif de garde à vue comme en témoigne dans l'émission « les pieds sur Terre » le Journaliste indépendant Clément interpellé à Sainte-Soline via une trace de PMC.

Avec ce marquage, même si vous n'avez rien fait, cela prouve que vous étiez présent-e. Or comme le souligne la Ligue des Droit d'Homme, en référence à l'article 34 de la Constitution, les règles pour rechercher les auteurs d'infraction pénale, relèvent de la loi et uniquement de la loi. Mais concernant les PMC il n'y a pas de loi ! Les PMC constituent ainsi une nouvelle atteindre à la liberté de manifester.

Enfin, il existe également des dispositifs de marqueurs fixes dits « expérimentaux », en service depuis 2011 selon le site officiel de la gendarmerie. Quelle est la date limite d'une expérimentation ? Il s'agit de sortes de douches placées au dessus d'une porte, qui vaporisent un spray de produit de marquage codé sur la personne entrant par effraction dans un lieu. La gendarmerie parle de 111 sites équipés, qui auraient « démontré leur pouvoir de dissuasion », notamment dans des commerces.

111 sites dans 17 départements métropolitains, qui fonctionnent comme des douches pour marquer des indésirables. Sordide.

(post de Contre Attaque)

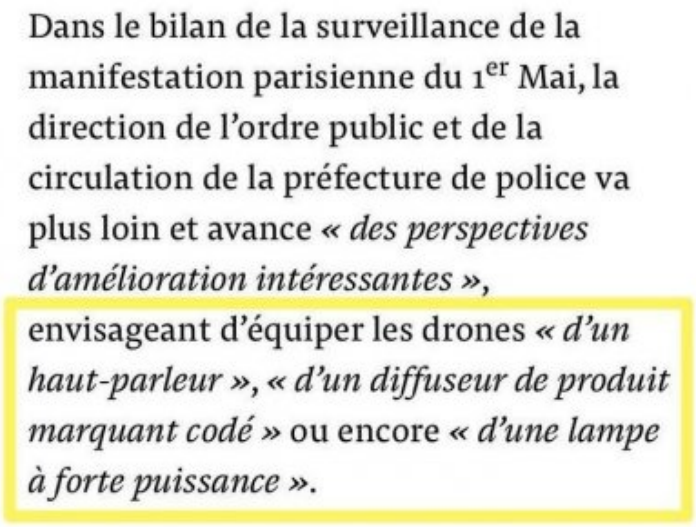
Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

Nouveaux dispositifs de l'industrie de la sécurité, par Mathieu Rigouste

- **La police du futur - De la surveillance généralisée à l'autocontrôle** : Robots autonomes, officiers connectés, reconnaissance génomique... l'innovation dans les équipements et moyens mis au service de la police ne semble pas connaître de limites. États et entreprises privées avancent main dans la main, développant un

arsenal sécuritaire hypertechnologique, dans le cadre d'un marché mondialisé en forte croissance. Ces nouveaux dispositifs directement calqués sur le matériel militaire brillent d'ailleurs davantage par les bénéfices qu'ils permettent d'engranger que par leur efficacité réelle et leur infaillibilité technique. Ils sont toutefois rendus acceptables - voire désirables - aux yeux des populations par le biais d'une novlangue publicitaire et d'un marketing particulièrement soignés. **La « police du futur » ouvre des perspectives orwelliennes : il ne s'agit pas seulement d'« optimiser » les équipements et les méthodes des forces de l'ordre, mais bien de poser les jalons d'un véritable panoptique policier qui a pour objectif d'aboutir à l'autocontrôle des populations.**

- **Des jeux dont vous êtes le cobaye - Business sécuritaire et spectacle olympique** : Depuis plusieurs années, les mobilisations contre l'organisation des grands événements sportifs se multiplient à travers le monde. A l'approche des Jeux Olympiques et Paralympiques (JOP) de Paris, qui se dérouleront du 26 juillet au 8 septembre 2024, les opposants mettent notamment en cause leurs conséquences écologiques et leur coût financier. Mais un autre aspect inquiète les observateurs : le déploiement massif des technologies sécuritaires. **Videosurveillance algorithmique, centres de supervision urbains, drones et matériels antidrones, robots de contrôle et d'intervention, interfaces homme-machine, armements plus ou moins automatisés, technologies de reconnaissance faciale en temps réel : les industries de la sécurité entendent bien profiter de cet événements planétaire pour expérimenter et promouvoir leurs nouveaux dispositifs**. En collaboration étroite avec les pouvoirs publics, comme a pu le constater le chercheur Mathieu Rigouste lors de la dernière édition de Milipol, le "salon mondial de la sûreté intérieure des Etats".


Dans le bilan de la surveillance de la manifestation parisienne du 1er Mai, la direction de l'ordre public et de la circulation de la préfecture de police va plus loin et avance « *des perspectives d'amélioration intéressantes* », envisageant d'équiper les drones « *d'un haut-parleur* », « *d'un diffuseur de produit marquant codé* » ou encore « *d'une lampe à forte puissance* ».

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

Drones avec HP, lampe, diffuseur de marquant codé, pour commencer...

"**Dans le bilan de la surveillance de la manifestation parisienne du 1er Mai, la direction de l'ordre public et de la circulation de la préfecture de police avance « des perspectives d'amélioration intéressantes », envisageant d'équiper les drones « d'un haut-parleur », « d'un diffuseur de produit marquant codé » ou encore « d'une lampe à forte puissance »**.

Cet empressement du ministère de l'Intérieur contraste avec le flou ayant entouré jusqu'à il y a encore peu de temps les pratiques des forces de l'ordre en la matière. Comme le rappelle La Quadrature du Net, les drones ont en effet été longtemps utilisés hors de tout cadre légal. L'association de défense des libertés numériques, qui s'est jointe au recours, avait même obtenu l'interdiction de leur utilisation par le Conseil d'État au mois de décembre 2020, entraînant la condamnation du ministère de l'intérieur par la Commission nationale de l'informatique et des libertés (

CNIL).
Le gouvernement avait tenté de régulariser sa situation lors du vote de la loi [dite] « sécurité globale » du 25 mai 2021. Mais les articles relatifs aux drones avaient dans la foulée été censurés par le Conseil constitutionnel, et ce dû aux trop faibles garanties apportées au regard des libertés individuelles mises en jeu.
Le gouvernement avait très vite revu sa copie et intégré un nouveau cadre légal de l'utilisation des drones à la loi « responsabilité pénale et sécurité intérieure » adoptée le 18 novembre 2021. Le Conseil constitutionnel avait cette fois validé le dispositif mais celui-ci nécessitait encore la prise d'un décret fixant ses conditions d'application concrètes."
[...]

"« Les drones ont une capacité de visualisation sur un rayon de 600 mètres. La taille des cartes mémoires embarquées est de 200 Go, soit environ 50 DVD, ajoute l'un des mémoires des requérants. Il est donc fondamental que l'usage des drones soit encadré par les textes de la manière la plus pointilleuse possible, de façon prévisible pour les administrés, ne laissant quasiment aucune marge de manoeuvre opérationnelle aux préfets, comme l'exige le droit de l'Union européenne. »
« Les six finalités toutes vagues et imprécises, et leur agrégation, permettent en réalité l'usage des caméras aéroportées dans tout type de situation ou un risque classique de trouble a l'ordre public est susceptible d'être commis, ou lorsqu'il existe un risque pour la sécurité des personnes et des biens, et cela le cas échéant pour une durée de trois mois renouvelable », estime Me Soufron.
« **D'ores et déjà, ainsi qu'il ressort des écritures en défense, la préfecture de police réclame la possibilité de diffuser des produits marquant par drones, avertit encore le recours. Ensuite vont se déployer des outils de reconnaissance faciale permettant d'individualiser, de reconnaître et de suivre dans la durée les personnes filmées par les caméras.** »"

- Source : https://www.mediapart.fr/journal/france/160523/un-recours-devant-le-conseil-d-etat-pour-stopper-l-envol-des-drones

Transformer les objets connectés en mouchards : la surenchère sécuritaire du gouvernement

- **Transformer les objets connectés en mouchards : la surenchère sécuritaire du gouvernement** : Communiqué de l'Observatoire des Libertés et du Numérique, 31 mai 2023

(...) En clair, il s'agira par exemple pour les enquêteurs judiciaires de géolocaliser une voiture en temps réel à partir de son système informatique, d'écouter et enregistrer tout ce qui se dit autour du micro d'un téléphone même sans appel en cours, ou encore d'activer la caméra d'un ordinateur pour filmer ce qui est dans le champ de l'objectif, même si elle n'est pas allumée par son propriétaire. Techniquement, les policiers exploiteront les failles de sécurité de ces appareils (notamment, s'ils ne sont pas mis à jour en y accédant, ou à distance) pour installer un logiciel qui permet d'en prendre le contrôle et transformer vos outils, ceux de vos proches ou de différents lieux en mouchards.

L'activation à distance pourra concerner toutes les personnes suspectées d'avoir commis un délit puni de cinq années de prison

(...) Concernant la technique de géolocalisation des objets connectés, le spectre est encore plus large puisque l'activation à distance pourra concerner toutes les personnes suspectées d'avoir commis un délit puni de cinq années de prison, ce qui - en raison de l'inflation pénale des lois successives - peut aller par exemple du simple recel, à la transmission d'un faux document à une administration publique, ou le téléchargement sans droit de documents d'un système informatique.

Surtout, l'histoire nous a démontré qu'il existait en la matière un « effet cliquet » : une fois qu'un texte ou une expérimentation sécuritaire est adopté, il n'y a jamais de retour en arrière. À l'inverse, la création d'une mesure intrusive sert généralement de base aux extensions sécuritaires futures, en les légitimant par sa seule existence. Un exemple fréquent est d'étendre progressivement des dispositions initialement votées pour la répression d'un crime choquant à d'autres délits. Le fichage génétique (FNAEG) a ainsi été adopté à l'encontre des seuls auteurs d'infractions sexuelles, pour s'étendre à quasiment l'ensemble des délits : aujourd'hui, 10% de la population française de plus de 20 ans est directement fichée et plus d'un tiers indirectement.

(...) Il s'agit d'un pas de plus vers une dérive totalitaire qui s'accompagne au demeurant d'un risque élevé d'autocensure pour toutes les personnes qui auront - de plus en plus légitimement - peur d'être enregistrées par un assistant vocal, que leurs trajets soient pistés, et même que la police puisse accéder aux enregistrements de leurs vies

(...)

En visite aux « nuits de l'AN2V », le lobby de la vidéosurveillance

En visite aux « nuits de l'AN2V », le lobby de la vidéosurveillance - Il a fallu débourser 180Euros et s'arracher à la torpeur de ce début d'été pour gagner le droit de s'attabler incognito au beau milieu du « milieu » français de la vidéosurveillance policière. L'AN2V, ou association nationale de la vidéoprotection, tenait l'une de ses « nuits de l' AN2V » à Paris le 27 juin dernier. Événement biennal, les « nuits » sont le moment le plus people de cette association de fabricants, de distributeurs, d'intégrateurs, bref de marchands des milliers de caméras de surveillance installées à grands frais dans nos villes et villages.

Ils se font croire qu'ils croient encore en la démocratie

(...) Au fond, les nuits de l'AN2V sont un peu comme un confessionnal où les acteurs de la Technopolice sont venus ressasser leurs péchés pour mieux laver leur mauvaise conscience, un moment étrange où l'aveu implicite permet d'entretenir le déni. Faute secrètement avouée, à moitié pardonnée. Après ce bref moment de catharsis et de contrition silencieuse, chacun pourra s'en retourner à sa routine consistant à maximiser les profits liés à l'expansion des marchés de la surveillance. Plutôt qu'un paradoxe, et n'en déplaise à Charouqui, le gargarisme de démocratie auquel j'ai assisté ce soir révélerait donc l'un des mécanismes par lesquels les régimes libéraux contemporains « basculent », à savoir la déculpabilisation des élites et la production d'une irresponsabilité collective par la mise en scène des valeurs démocratiques. **Des représentants commerciaux aux donneurs d'ordre administratifs en passant par les parlementaires, les hauts-fonctionnaires ou les ministres, nombreux sont ceux qui, en participant à ces événements rituels, se font croire qu'ils croient encore en la démocratie. Peut-être même se convainquent-ils ainsi qu'ils peuvent faire ce qu'ils font, c'est-à-dire déployer des technologies toujours plus sophistiquées de contrôle social, tout en agissant en son nom. Tandis que l'extrême droite s'affirme de manière toujours plus décomplexée, ces processus grâce auxquels les élites libérales gèrent la dissonance cognitive induite par leur complicité objective avec la spirale autoritaire en cours forment l'un des rouages les plus efficaces du fascisme qui vient.**

Robots de surveillance autonome

Aux USA des robots de surveillance autonomes K5 filment et enregistrent à 360 degrés, et commencent à patrouiller dans l'Ohio.

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

Le Knightscope K5 Autonomous Data Machine a déjà 10 ans.

Parmi les capteurs utilisés, un capteur de reconnaissance optique de caractères (OCR), qui scanne les textes tout autour, les numérise, et les convertit en données, afin de les comparer avec une base de données, la "Hot List" - ce qui permet de savoir si tel ou tel mot est "sensible".

Le K5 utilise aussi des caméras haute définition - 360 degrés, des capteurs thermiques qui détectent et mesurent les différences de températures en temps réel, des micros haute précision qui capturent les sons alentour et des détecteurs ultrasons pour mesurer la vitesse (et les distances) des objets environnants. Enfin, un système de détection "radar" utilise les ondes radios pour déterminer l'altitude, la position, la direction et la vitesse de ces objets.

Le robot intelligent possède des capteurs et des outils GPS, qui lui permettent de cartographier, en 3D, son environnement.

Muni de toutes ces données, le K5 passe tout ça à la moulinette, **dans un "moteur d'analyse prédictive", un filtre (un algorithme) utilisant des bases de données d'entreprises, du gouvernement, ainsi que des "bases de données publiques" issues du crowdsourcing.**

https://www.futura-sciences.com/tech/actualites/robotique-k5-robot-vigile-voit-entend-sent-odeurs-50922/

Sa mission : patrouiller dans les lieux publics ou les bâtiments et donner l'alerte au moindre événement suspect. Il ne s'agit pas du thème d'un énième film de science-fiction, mais d'un programme tout ce qu'il y a de plus réel. Le robot K5 a été conçu aux États-Unis par la société Knightscope, qui commencera l'année prochaine un test pilote avec plusieurs partenaires dans la Silicon Valley (Californie). Le K5 peut se déplacer de façon autonome, voir à 360°, y compris la nuit, et lire les plaques d'immatriculation. L'idée est de s'en servir pour surveiller notamment des campus, des centres commerciaux, des écoles, des parkings ou des quartiers. Il jouera les agents de sécurité, l'arme en moins (,pour l'instant, c'est nous qui ajoutons cette parenthèse).

(...)

Des microphones analyseront les bruits ambiants afin de détecter par exemple de cris ou des coups de feu. Il est aussi question d'utiliser les caméras pour faire de la reconnaissance faciale en s'appuyant sur des bases de données. Enfin, K5 sera aussi équipé de capteurs pour détecter les radiations ainsi que les émanations chimiques et bactériologiques. Ce flux d'informations sera traité en temps réel par un logiciel prédictif qui pourra

déclencher l'envoi d'une alerte à l'opérateur humain chargé de contrôler le robot. L'ensemble des données collectées durant un cycle de surveillance sera sauvegardé et transmis aux opérateurs concernés

Fichage : Smart Police d'Edicia, le logiciel à tout faire des polices municipales

- **Smart Police d'Edicia, le logiciel à tout faire des polices municipales**

Dans le cadre d'une enquête sur les technologies de police prédictive dont nous vous reparlerons très bientôt, La Quadrature s'est intéressée de près à Edicia. Cette startup est peu connue du grand public. Elle joue pourtant un rôle central puisqu'elle équipe des centaines de polices municipales à travers le pays. Son logiciel Smart Police, dont nous avons obtenu le manuel d'utilisation, permet de faire un peu tout et n'importe quoi. Loin de tout contrôle de la CNIL, Smart Police encourage notamment le fichage illégal, une pratique policière en vogue...

(...)

On le comprend au regard de ces descriptions, Smart Police comporte un risque important de voir consignées des données identifiantes, et donc là encore de conduire à des opérations de fichage illégal. Notamment, il ne semble pas respecter le cadre réglementaire s'agissant des traitements automatisés utilisés par les polices municipales pour gérer les mains courantes, puisque ce dernier exclut la prise de photographies

(...)

Nos inquiétudes à ce sujet sont évidemment renforcées par des révélations récentes. La presse locale s'est récemment faite l'écho de pratiques de policiers municipaux dans une commune de la région PACA consistant à échanger, sur des boucles WhatsApp privées et à partir de leurs smartphones personnels, des données sensibles relatives à des personnes : images extraites de la vidéosurveillance, photos des personnes contrôlées, plaques d'immatriculation, pièces d'identité, etc. **Des pratiques totalement illégales mais dont on peut supposer qu'elles sont monnaie courante, non seulement au sein des polices municipales mais aussi au sein de la police nationale.**

(...)

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

DIVERS

- Bientôt Terminator ? : **Et voilà ChatGPT dans un robot-chien de Boston Dynamics** - Des ingénieurs ont trouvé le moyen d'activer ChatGPT dans un robot quadrupède fabriqué par Boston Dynamics. On peut ainsi le diriger à voix haute.
- **Tribune : «** Attachés aux libertés fondamentales dans l'espace numérique, nous défendons le droit au chiffrement de nos communications » - Cette tribune a été rédigée suite à la publication de notre article sur la criminalisation des pratiques numériques des inculpé·es de l'affaire du 8 décembre. Cette tribune a été signée par plus de 130 personnes et organisations et publiée hier sur le site du journal Le Monde.

- **Les** JO 2024, médaille d'or de la surveillance de masse - Les Jeux olympiques de 2024 consacreront des centaines de millions d'euros aux caméras, drones et policiers pour surveiller Paris. Des mesures d'exception qui risquent de perdurer longtemps après la compétition. (...) « Plus on va s'approcher des JO, plus on va saturer l'espace public de policiers », prévenait en avril le préfet de police de Paris, Laurent Nuñez (...) « Les Jeux olympiques et paralympiques sont avant tout un spectacle sécuritaire, observe l'anthropologue Matheus Viegas Ferrari, qui rédige sa thèse sur les Jeux de Paris 2024. Après les guerres, c'est là qu'est dépensé le plus gros budget sécuritaire. » (...)
- **L'Assemblée adopte l'activation à distance des appareils électroniques** - La semaine dernière, l'Assemblée nationale a adopté le projet de loi d'orientation et de programmation du ministère de la justice pour les années 2023-2027. Parmi de multiples dispositions, ce texte prévoit l'introduction dans le droit français la possibilité pour la police d'activer des appareils et objets électroniques à distance, que ce soit les fonctionnalités de géolocalisation, des micros ou des caméras.(...)
- **La police prédictive en France : contre l'opacité et les discriminations, la nécessité d'une interdiction** - Après plusieurs mois d'enquête, dans le cadre d'une initiative européenne coordonnée par l'ONG britannique Fair Trials, La Quadrature publie aujourd'hui un rapport sur l'état de la police prédictive en France. Au regard des informations recueillies et compte tenu des dangers qu'emportent ces systèmes dès lors qu'ils intègrent des données socio-démographiques pour fonder leurs recommandations, nous appelons à leur interdiction. (...) En effet, les scores de risque sont possiblement corrélés à un taux de chômage ou de pauvreté important, ou encore à un taux élevé de personnes nées en dehors de l'Union européenne dans le quartier considéré. Et ce d'autant plus que l'on sait que, pour PAVED, parmi les données pertinentes pour l'établissement des « prédictions », on retrouve les indicateurs suivants : nationalité et données d'immigration, revenus et composition des ménages ou encore niveau de diplôme. Autant de variables qui risquent de conduire à cibler les populations les plus précarisées et les plus exposées au racisme structurel. (...) les logiciels de police prédictive soulèvent un important risque d'effet d'auto-renforcement et donc d'une démultiplication de la domination policière de certains quartiers (surveillance, contrôle d'identité, usages de pouvoirs coercitifs). (...) La police prédictive produit ainsi une prophétie auto-réalisatrice en concentrant des moyens importants dans des zones déjà en proie aux discriminations et à la sur-policiarisation.
- **La technopolice à l'oeuvre dans les villes et villages** - Les équipements de vidéosurveillance sont étendus vers des technologies de plus en plus inquisitrices. Le nombre croissant des usages qui en sont fait et leur combinaison renforcent le pistage.
- **Contre les obsessions sécuritaires, attaquons les** JO du contrôle ! - Liste des entreprises qui se font de la maille avec le business du réarmement et de la surveillance.
- **La France crée un fichier des personnes trans** - Révélé et dénoncé par plusieurs associations de défense des droits des personnes transgenres, un récent arrêté ministériel autorise la création d'un fichier de recensement des changements d'état civil. Accessible par la police et présenté comme une simplification administrative, ce texte aboutit en réalité à la constitution d'un fichier plus que douteux, centralisant des données très sensibles, et propice à de nombreuses dérives. Le choix de créer un tel fichier pose d'immenses problèmes aussi bien politiquement que juridiquement.

Chiens robots policiers à NY

A New York, la distopie est désormais réalité avec des premiers policiers robots, sous forme de "chiens". L'histoire ne dit pas encore si ces policiers sans âme font aussi dans le contrôle au faciès et dans le crime raciste...

vidéo : https://fb.watch/m6AnMkHMBk/

(post de CND)

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

™ æúîÿ îûñ æîóò Öö : üý öúö òÿ ùî ü úö öüû ñ ïò ïöù

https://greenwashingeconomy.com/smart-and-safe-city-optimiser-soumission-betail/

« Les techniques policières, qui se développent à une cadence extrêmement rapide, ont pour fin nécessaire la transformation de la nation tout entière en camp de concentration. » - Jacques Ellul, La Technique ou l'Enjeu du siècle, 1954.

G ßî « æîóò îûñ æúîÿ Öö » (ýîÿ àî õöò åöôü ò)

Le marché mondial des « Smart Cities » constitue l'un des grands chantiers de cette transformation du pouvoir policier. Le concept a émergé au début des années 2000 comme projet de gestion numérique centralisée de l'espace public : réseaux de transport, éclairage, circulation, pollution et bien sûr systèmes de sécurité, dont l'enrobage publicitaire est assuré par la dénomination de « Safe City ».
Mais comme le note le chercheur Antoine Courmont, la globalisation d'un premier modèle de « Smart City » a échoué au début des années 2010. « [Les entreprises technologiques] se sont trouvées confrontées à la complexité du fonctionnement des villes difficilement commensurables par le biais de données et d'algorithmes[1]. » Selon Olivier Tesquet, la « Safe City » est en train de tout faire pour résoudre ce problème. « **Aux quatre coins du monde, la rente sécuritaire permet de conquérir le pouvoir ou de le conserver, et il est dès lors beaucoup plus simple de vendre des solutions clés en main à des collectivités intéressées. Ainsi, on voit Huawei équiper généreusement Belgrade en milliers de caméras boostées à la reconnaissance faciale, ou Thales proposer son modèle à Mexico aussi bien qu'à Nice. Là où la "Smart City" était un néologisme dépolitisé, la "Safe City" lui rend sa raison d'être : la surveillance et le contrôle social**[2]. »

Ce processus fait face à des contradictions institutionnelles des résistances populaires. En France, alors que la Région Sud avait prévu de mettre en place des portiques à reconnaissance faciale à l'entrée de deux lycées de quartiers populaires à Nice et à Marseille, le tribunal administratif et la CNIL ont interdit l'expérimentation sous la pression de collectifs comme la Quadrature du Net, de syndicats de professeurs et associations de parents d'élèves.
Dès l'apparition de la notion de « Safe and Smart City », un rapport de la Commission Nationale de l'Informatique et des Libertés (CNIL) avait dénoncé ce programme de ville « pilotée depuis un unique tableau de bord, avec l'algorithme comme grand ordonnateur », mettant en cause « un système centralisé qui risque de laminer un certain nombre de libertés[3] ». La « Safe and Smart City » désigne tout à la fois un programme, un mythe politique et une plateforme publicitaire où l'habitant est mis au centre pour « envisager ses habitudes et comportements comme autant d'informations à gérer ou de problèmes à résoudre[4] ». Comme l'expliquait le directeur de la communication

du GICAT, elle est au centre des stratégies de « Recherche et développement » des industries de la guerre et du contrôle. « Notre coeur de métier c'est la Safe City », assure-t-il, même si « l'humain reste au coeur de l'opération* ».

« L'ensemble des données recueillies par les caméras a vocation à alimenter un big data de la tranquillité publique [...] afin de fournir aux forces de l'ordre une aide à la décision, voire dans certains cas une capacité prédictive »

La « Safe and Smart City » s'apparente à une gestion de flux d'informations, de marchandises, de risques et de populations. Laurent Denizot, chargé de la « Safe City » au Conseil des industriels de la confiance et de la sécurité (CICS), développe ainsi l'idée de conjuguer ces flux à travers un « continuum numérique permanent[5] ». La filière française des industries de sécurité est regroupée autour du développement des « Safe Cities » depuis 2014 sous l'impulsion de l'État. Paris et Nice ont servi de premiers « démonstrateurs » pour une « plateforme connectée de sécurité du quotidien », tandis que Marseille constitue un grand terrain d'expérimentation avec le projet d'en faire la « première "Safe City" du continent[6] ». Un partenariat de coproduction a été mis en place avec des entreprises comme Atos, l'un des leaders mondiaux sur le marché des technologies digitales et numériques. La firme expérimente « des réseaux de communication de défense qui permettent aux acteurs de terrain de parler entre eux ». Le vaste réseau de vidéosurveillance marseillais devait être centralisé au sein d'un Centre de supervision urbain (CSU) développé par Engie Ineo. « L'ensemble des données recueillies par les caméras a vocation à alimenter un big data de la tranquillité publique [...] afin de fournir aux forces de l'ordre une aide à la décision, voire dans certains cas une capacité prédictive », expliquait Caroline Pozmentier-Sportich, à l'époque maire adjointe à la sécurité publique de Marseille[7]. D'autres villes servent d'incubateurs pour les nouvelles technologies de contrôle social. À Valenciennes, l'entreprise chinoise Huawei a fourni gratuitement à la police municipale ses technologies de « vidéosurveillance intelligente » prétendant pouvoir déceler automatiquement les comportements déviants à la norme. La société IBM a procédé de la même manière dans le cadre d'un marché public à Toulouse, tandis qu'IDEMIA et Thales mettaient en pratique leurs systèmes de « vision assistée par ordinateur » en collaboration avec la Ville de Paris.

Des dizaines de « Safe and Smart Cities » existent déjà en Chine ou dans la péninsule Arabique. On y observe des régimes de concurrence entre centres de décision multiples et réticulaires plutôt qu'une forme de gouvernement type Big Brother gérant la ville de manière infaillible[8].

Cette dynamique est aussi confrontée à des dénonciations dans le monde entier. En France, elle est critiquée par différents collectifs et associations et elle a vu émerger des groupes d'enquête et d'action comme la Quadrature du Net et la campagne participative « Technopolice[9] » engagée en 2019. Cette dernière a permis de récolter et d'analyser de nombreux documents, elle a construit des collaborations entre groupes d'enquête et activistes, elle a lancé des recours en justice et mené des actions de rue.

Critique d'une transparence sans fin

Critique d'une transparence sans fin - L'intelligence des villes, Tyler Reigeluth

[Bonnes Feuilles]

Smartphone, smartcar, smartbuilding, smartlight, smartcooling et même smart dust, tout ce qui nous entoure semble devenir intelligent, smart, jusqu'à la ville de demain, la smart city promue par les ingénieurs et les politiques urbaines. La smart city se présente comme un nouvel espace de vie accessible et régulable en temps réel, totalement transparent et saisissable. Un nouvel espace qui répondra à tous les enjeux de notre temps, écologiques, sociaux, politiques et économiques.

Mais quelle est la part de fantasmes dans ces visions post-cybernétiques ?

Quels mondes produisent-elles ? Pour qui et pour quoi ?

Contre une vision mystifiée et inerte de l'intelligence des villes, en mobilisant Henri Lefevbre, Gilbert Simondon,

mais aussi J. G. Ballard et Italo Calvino, ce livre entend redonner à l'intelligence toute sa dimension matérielle, faire voir de quoi son image de transparence est faite. **Il se propose de fragmenter et d'épaissir la notion d'intelligence, pour défaire un discours contemporain sur l'intellience des villes qui ne semble tenir à rien, ni à la ville ni à ses habitant"es et s'imposer partout**.

(...)

La vidéosurveillance automatisée, déjà gagnante de la Coupe du monde de rugby en France

- **La vidéosurveillance automatisée, déjà gagnante de la Coupe du monde de rugby en France**

"Il est possible de douter du caractère réellement expérimental du recours à ces dispositifs de surveillance. Ce constat est d'autant plus préoccupant qu'il sera difficile de tirer un bilan à ce titre après l'organisation de ces grands rassemblements sportifs. En effet, en l'absence (évidemment souhaitable) de tout événement dramatique, on ne manquera sans nul doute de saluer l'efficacité de ces outils â€" alors même que cette réussite serait sans doute expliquée par bien d'autres facteurs â€" tandis que s'il devait advenir un quelconque incident, on soulignerait la pertinence de renforcer ces dispositifs de surveillance et de contrôle.

Ainsi, le dispositif technosécuritaire aurait toujours raison et ce d'autant plus que l'organisation de telles compétitions peut apparaître comme une « vitrine sécuritaire » pour les États concernés aux yeux du monde.

L'accoutumance à ces outils, comme l'effet cliquet â€" selon lequel il est difficile de revenir en arrière une fois un cap passé â€" rendent tout retour en arrière encore plus invraisemblable."

(...)

(note : ces dispositifs avaient déjà été déployé auparavant, illégalement)

Chronique de la technopolice : 8 ans de vidéosurveillance biométrique illégale, drones partout, reconnaissance faciale généralisée, surveillance par algorithmes des allocataires de la CAF, fichages illégaux par les polices municipales, la CNIL complice du fichage administratif...

LA SURVEILLANCE AVEC INTELLIGENCE ARTIFICIELLE MAINTENUE APRÈS LES JEUX

OLYMPIQUES

Ce n'est malheureusement pas une surprise, mais l'intervention de la Ministre des Sports confirme la fuite en avant annoncée.

Le gouvernement compte « expérimenter » la vidéosurveillance algorithmique appuyée par Intelligence Artificelle lors des Jeux Olympiques. Une technologie ultra-liberticide permettant de suivre et d'identifier tous les individus en temps réel dans l'espace public. Les autorités avaient promis juré craché que cela ne durerait que le temps des JO, et pas après. Paroles de macronistes.

Ce dimanche 24 septembre, la ministre des Sports Amélie Oudéa-Castéra était interrogée sur la chaîne France 3 à ce sujet. Pour une fois, la journaliste lui pose une question pertinente :

« Les lois d'exception en France elles sont souvent rentrées dans le droit commun. Est-ce que ce dispositif là, la vidéoprotection grâce à l'intelligence artificielle, vous vous engagez à ce qu'elle ne soit plus mise en place à l'issue de son expérimentation lors des Jeux Olympiques ? »

Réponse de la ministre : « Ce que prévoit le texte de loi, c'est qu'il y ait une évaluation qui soit menée, c'est une expérimentation sous le contrôle de la CNIL, et il n'y aura aucune prolongation sans une évaluation [...] de son efficacité »

Face à cette réponse pleine de langue de bois, la journaliste relance : « Donc il est possible que cette loi devienne pérenne ? »

La ministre crache le morceau : « Si ça fait ses preuves et entouré des garanties [...] les français attendent de nous qu'on agisse pour leur sécurité et qu'on fasse usage des moyens nouveaux, y compris numériques, pour favoriser cette sécurité. »

C'est confirmé, les Jeux Olympiques seront bien une expérimentation gigantesque de technologies liberticides qui seront ensuite généralisées. La compétition prévue l'année prochaine est l'occasion d'une accélération brutale des technologies de surveillance. Un « projet de loi JO 2024 » avait été déposé en tout discrétion, pendant les fêtes de fin d'année 2022.

L'article 7 du projet autorisait « à titre expérimental » l'utilisation en temps réel de systèmes d'intelligence artificielle pour analyser les images des drones et des caméras de surveillance. Une première en France et sans doute en Europe.

La surveillance dite « automatisée » ou « algorithmique », ce sont des logiciels qui analysent en continu les milliers d'images de surveillance et envoient une alerte à la police s'ils détectent un « comportement suspect ». Un individu ou un groupe peut être identifié, tracé, ses faits et gestes analysés automatiquement dans l'espace public. À terme, ces technologies permettent par exemple l'identification par reconnaissance faciale instantanée et la massification de la vidéoverbalisation. Et tout cela, sans vrai débat public, sans consulter la population.

En matière de répression et de reculs des libertés, l'exception finit toujours par devenir la norme

En matière de répression et de reculs des libertés, l'exception finit toujours par devenir la norme. Les tests ADN autorisés il y a une vingtaine d'années devaient rester exceptionnels : uniquement dans le cadre d'enquêtes criminelles les plus graves, en particulier la pédocriminalité et les assassinats les plus violents. Ils se sont immédiatement généralisés. Aujourd'hui, le moindre tagueur ou manifestant arrêté est obligé de donner son ADN. Résultat ? Plusieurs millions de français fichés.

De même pour l'état d'urgence, dont les mesures "exceptionnelles" devaient être limitées uniquement après les attentats de 2015 pour lutter contre le terrorisme, et qui sont finalement rentrées dans le droit commun. Les mesures de l'état d'urgence ont d'ailleurs été utilisées contre le mouvement écologistes puis pour interdit des militants de manifester. Également, la plupart des mesures liberticides « temporaires » de « l'état d'urgence sanitaire » sont

devenues pérennes.

Empêchons les murs de se refermer avant qu'il ne soit trop tard

Idem pour les dissolutions, procédures d'exceptions qui frappent à présent des médias indépendants, des mouvements écologistes, des associations musulmanes en grand nombre. Comme l'utilisation de forces anti-terroristes, récemment déployées contre des civils après la mort de Nahel. On peut malheureusement multiplier les exemples à l'infini. **Il n'y a pas de retour en arrière quand les libertés reculent.**

Le « meilleur des mondes » que nous préparent les gouvernants est une prison à ciel ouverte ou tous les possibles seront réprimés. Empêchons les murs de se refermer avant qu'il ne soit trop tard.

(post de Contre Attaque)

Le règlement européen sur l'IA n'interdira pas la surveillance biométrique de masse

- **Le règlement européen sur l'**IA n'interdira pas la surveillance biométrique de masse

Le 8 décembre 2023, les législateurs de l'Union européenne se sont félicités d'être parvenus à un accord sur la proposition de règlement tant attendue relative l'intelligence artificielle (« règlement IA »). Les principaux parlementaires avaient alors assuré à leurs collègues qu'ils avaient réussi à inscrire de solides protections aux droits humains dans le texte, notamment en excluant la surveillance biométrique de masse (SBM).

Pourtant, malgré les annonces des décideurs européens faites alors, le règlement IA n'interdira pas la grande majorité des pratiques dangereuses liées à la surveillance biométrique de masse. Au contraire, elle définit, pour la première fois dans l'UE, des conditions d'utilisation licites de ces systèmes. Les eurodéputés et les ministres des États membres de l'UE se prononceront sur l'acceptation de l'accord final au printemps 2024.
(...)

La France s'est battue pour préserver ou étendre les pouvoirs de l'État afin d'éradiquer notre anonymat dans les espaces publics et pour utiliser des systèmes d'intelligence artificielle opaques et peu fiables afin de tenter de savoir ce que nous pensons

Cela signifie que le règlement IA autorisera de nombreuses formes de reconnaissance des émotions - telles que l'utilisation par la police de systèmes d'IA pour évaluer qui dit ou ne dit pas la vérité - bien que ces systèmes ne reposent sur aucune base scientifique crédible. Si elle est adoptée sous cette forme, le règlement IA légitimera une pratique qui, tout au long de l'histoire, a partie liée à l'eugénisme.
(...)
À l'approche des Jeux olympiques et paralympiques qui se tiendront à Paris cet été, la France s'est battue pour préserver ou étendre les pouvoirs de l'État afin d'éradiquer notre anonymat dans les espaces publics et pour utiliser des systèmes d'intelligence artificielle opaques et peu fiables afin de tenter de savoir ce que nous pensons. Les gouvernements des autres États membres et les principaux négociateurs du Parlement n'ont pas réussi à la contrer dans cette démarche.
En vertu du règlement IA, nous serons donc tous coupables par défaut et mis sous surveillance algorithmique, l'UE ayant accordé un blanc-seing à la surveillance biométrique de masse. Les pays de l'UE auront ainsi carte blanche pour renforcer la surveillance de nos visages et de nos corps, ce qui créera un

précédent mondial à faire froid dans le dos.