https://ricochets.cc/La-technopolice-c-est-la-ville-connectee-la-smart-city-chronique-de-la-numerisation-totalitaire-de-la-gestion-du-monde.html

La technopolice c'est la ville connectée, la smart city : chronique de la numérisation de la gestion totalitaire du monde

Publication date: mardi 19 juillet 2022

- Les Articles -

Copyright © Ricochets - Tous droits réservés

La technopolice ce n'est seulement les usages spécifiquement policier de technologies numériques et high-tech, c'est surtout un mode de gestion cybernétique généralisé des Etats et du capitalisme, qui s'applique à toute la société, aux masses comme aux individus ciblés.

La technopolice c'est le techno-monde administré

La technopolice c'est l'ensemble de la société connectée et de tous ses dispositifs de traçage, d'analyse, de surveillance et d'accumulation de données, c'est le techno-monde administré. Un techno-monde qui ne se contente pas de rendre la planète étouffante et invivable, mais qui veut aussi étouffer totalement les libertés sous couvert de sécurité et de gestion des désastres qu'il produit lui-même.
Survivre vaguement en imitant les machines qui nous surveillent de plus en plus étroitement, ou détruire le techno-monde pour vivre libre ?

L'Europe et ses Etats veulent imposer un pass numérique pour tout le monde, pour tout usage de la vie quotidienne !

Carta Academica : pourquoi un portefeuille numérique européen à marche forcée ? - Les institutions de l'Union européenne restent très actives sur le front du portefeuille d'identité numérique ou eIDAS Wallet, un dispositif aux conséquences majeures sur nos futurs modes de vie.
(...)

L'Europe s'active pour lancer le portefeuille d'identité numérique ou eIDAS Wallet

Pendant que l'Europe et le monde, encore en rémission du covid, ont les yeux tournés vers l'Ukraine, les institutions de l'Union européenne restent très actives sur un autre front : celui du portefeuille d'identité numérique ou eIDAS Wallet, un dispositif aux conséquences majeures sur nos futurs modes de vie. Qu'on en juge plutôt : **il s'agit de doter, d'ici 2030, au moins 80 % des citoyens européens d'un portefeuille rassemblant dans leur smartphone l'ensemble de leurs identités numériques, leurs données personnelles et autres justificatifs**. Le but : permettre à chacun de s'identifier dans des contextes très divers : payement en ligne, preuve des diplômes acquis, parcours de santé, et ce, d'une manière à chaque fois « contrôlée » par l'utilisateur.
(...)

Chaque Etat pourra déléguer à des entreprises privées la délivrance des identités numériques !

Et là, on écarquille les yeux, incrédule : car on apprend que désormais, chaque Etat pourra déléguer à des entreprises privées la délivrance des identités numériques ! Autrement dit, moyennant certaines garanties (comme le respect du Règlement général sur la protection des données, RGPD), des entreprises pourraient fournir des identités numériques régaliennes, notamment via l'identité Google, Facebook Connect, Apple ID ou les comptes Microsoft - précisément, ces entreprises qui sont régulièrement sanctionnées pour enfreindre la loi, abuser les internautes et asseoir leur position dominante. Question confiance, peut mieux faire !
(...)
Projet capital, donc, projet tentaculaire même, qui pose un jalon essentiel sur la route de la **numérisation intégrale de la vie sociale de chacune et chacun d'entre nous, de notre dossier sanitaire, jusque dans l'utilisation de nos clés électroniques de voiture**. Mais projet qui, loin de faire l'objet d'un débat public et d'une appropriation

citoyenne, suit une marche forcée qui nous mettra toutes et tous, très vite, devant le fait accompli.
(...)
Quels sont les buts et finalités de cette numérisation intégrale de la vie sociale ? Quel modèle de société ce projet favorise-t-il ? La fluidification des interactions marchandes justifie-t-elle cette numérisation à marche forcée de tous les aspects de notre vie sociale ?
(...)
En l'état, cet agenda met la charrue avant les boeufs, l'organe avant la fonction, la solution avant le problème : le wallet avant sa finalité. Les impacts, buts et intentions ne sont jamais mis sur la table ni, a fortiori, questionnés : on avance tête baissée. Pour notre part, avant même d'alerter sur les problèmes de faisabilité, de sécurité, de risques encourus par les utilisateurs, de liberté de choix ou de fracture numérique, nous voulons questionner la manière de faire elle-même, la procédure qui, telle qu'elle est en marche, court-circuite le plus élémentaire processus démocratique de discussion.
(...)

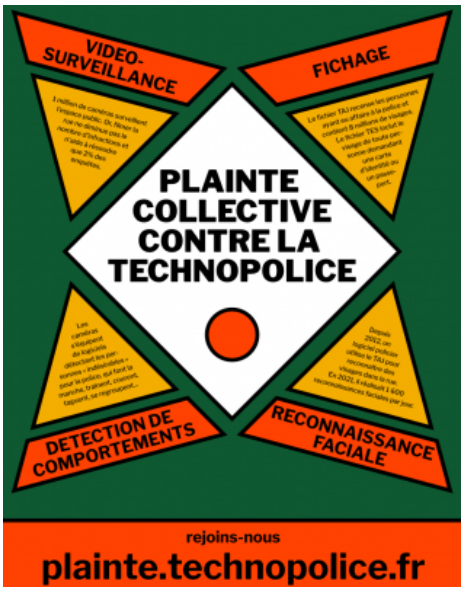
NOTE : on connaît la finalité de ce type de projet :

- fournir des données personnelles massives aux Etats et entreprises (pour allimenter Big data, IA, algorithmes...) et de nouvelles occasions de business aux entreprises capitalistes
- faciliter la surveillance et le fichage de tout le monde
- faciliter l'administration autoritaire des foules en cas de crises (comme pour le Covid-19), lesquelles vont se multiplier
- habituer tout le monde au bain techno-numérique pour empêcher tout retour « en arrière »

A rapprocher du passage, plus bas, sur la reconnaissance faciale généralisée.

Quand les flics prennent tes empreintes, ta photo et ton ADN de force

Quand les flics prennent tes empreintes, ta photo et ton ADN de force - Le 22 avril, plusieurs personnes en garde à vue qui refusent de donner leurs empreintes digitales, photo et ADN se voient contraintes physiquement par les flics à les donner. Premiers retours sur l'application de la loi du 24 janvier 2022, dans le cadre de la loi relative à la responsabilité pénale et à la sécurité intérieure



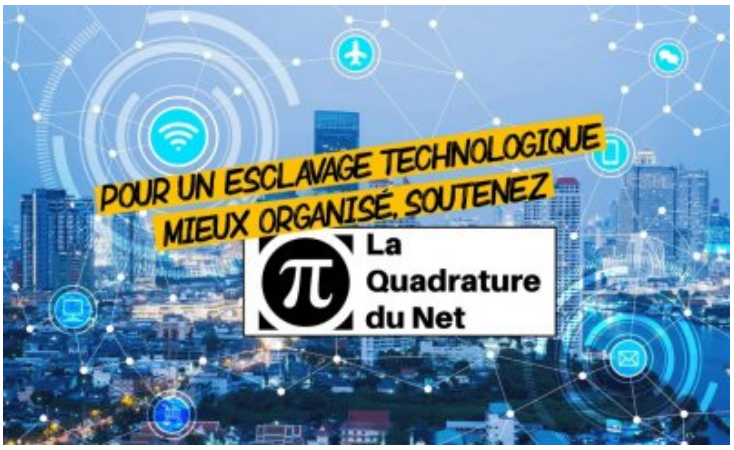
La technopolice c'est la ville connectée, la smart city : chronique de la numérisation de la gestion du monde

Les gardes-fou des institutions sont des dispositifs pour imposer l'acceptabilité progressive

Plainte collective contre la Technopolice

Plainte collective contre la Technopolice - Il y a 3 ans, La Quadrature du Net lançait l'initiative Technopolice pour recenser les nouvelles technologies policières installées dans nos villes. Aujourd'hui, la surveillance de nos rues est devenue totale, car ces technologies se renforcent les unes les autres : vidéosurveillance généralisée, fichage de masse, reconnaissance faciale et détection automatisée de comportements. Pour mettre un coup d'arrêt à cette surveillance totale, nous lançons une plainte collective contre le ministère de l'intérieur qui l'organise illégalement.

Rejoignez la plainte sur plainte.technopolice.fr. Vous y trouverez le détail de notre argumentaire et de la procédure. (...)



La technopolice c'est la ville connectée, la smart city : chronique de la numérisation de la gestion du monde
Un impossible techno-monde régulé, ou une autre société ?, avec donc de toutes autres techniques

Technopolice : l'escroquerie du citoyennisme numérique (par PMO et Tomjo)

Technopolice : l'escroquerie du citoyennisme numérique (par PMO et Tomjo)

Un texte que nous reproduisons depuis le site de PMO, initialement publié à cette adresse : https://www.piecesetmaindoeuvre.com/spip.php?page=resume&id_article=1712. De la même manière qu'il n'existe pas de bonne version de l'État (avec de bons dirigeants, etc.), il n'existe pas de bonne société technologique, de bon usage des technologies modernes. Les problèmes qu'elles posent leur sont intrinsèques, ils ne relèvent pas d'une mauvaise manière de les produire, d'une mauvaise manière de les utiliser, etc., mais de ce qu'impliquent par défaut leur production, leur usage, etc. Les individus et les associations qui tentent de faire accroire le contraire sont les idiots utiles de leur imposition. & quoi qu'ils en disent, ils participent à la perpétuation du désastre techno-industriel en cours. Au passage, on soulignera, en plus de ce que rappellent déjà PMO et Tomjo dans ce texte, que La Quadrature du Net est soutenue (financée ?) par l'Electronic Frontier Foundation (EFF), basée à San Francisco, créée par trois hommes dont le président fondateur de la Mozilla Foundation, qui est également l'investisseur historique de l'organisation Linden Research (à l'origine de la création du monde virtuel Second Life). Sachant que l' EFF est elle-même financée par d'autres richissimes fondations (dont la Silicon Valley Community Foundation, le Craigslist Charitable Fund, la Flora Family Foundation, liée à la célèbre marque d'informatique HP, et d'autres). La Quadrature est également soutenue (financée ?) par la Free Software Foundation créée par le célèbre militant du logiciel libre Richard Stallman ; Free Software Foundation qui bénéficie elle-même, entre autres et quelque peu paradoxalement, du soutien institutionnel d'Alibaba Group, Bloomberg et Google.

La Quadrature du net (QDN), association « pour un Internet libre, décentralisé et émancipateur » (tendance « RGPD »), était à Calais le 21 juin, Roubaix le 22 et Lille le 24, avec sa « Caravane de la Technopolice », afin d'alerter les

citoyens sur les technologies de surveillance de masse dans l'espace public, et de lancer contre celles-ci une plainte collective : « Partout sur le territoire français, la Smart City révèle son vrai visage : celui d'une mise sous surveillance totale de l'espace urbain à des fins policières. »

Ladite « Quadrature » â€" pourtant un working space d'ingénieurs, de juristes et d'experts â€" révèle ainsi qu'elle ne sait, ni ce qu'est la police ; ni ce qu'est la technopolice. Mais qu'attendre de gens qui ne voient même pas l'ineptie du jeu de mots qui leur sert d'enseigne. La « quadrature du cercle » qu'ils essaient de détourner par humour machinal étant le type même du problème irrésoluble.

Quoi que prétendent la QDN et ses experts, l'« Internet libre » et le « numérique inclusif » ne seront jamais qu'un oxymore et un pléonasme. Examen d'une escroquerie en association citoyenne.

(...)

En réduisant le sens du mot « technopolice » au seul maintien de l'ordre public par des moyens technologiques (QR code, caméras, reconnaissance faciale, etc.), la QDN réduit également la critique des technologies à la seule critique du sécuritaire. Son objectif étant de trier le bon grain numérique de l'ivraie despotique, et de nous vendre un « Internet libre ». (...)

Et ainsi la technopolice n'est pas le flicage des citoyens par des moyens technologiques, mais l'organisation technologique de la cité.

(...)

La safe city n'est qu'un aspect mineur de la smart city

La « technopolice » n'est donc pas née de la vidéo-surveillance intelligente, avec sa détection automatisée des comportements frauduleux et la reconnaissance faciale, à des fins de maintien de l'ordre. Elle ne sert pas d'abord des hommes en bleu, des brutes paranoïaques. La safe city n'est qu'un aspect mineur de la smart city, qui est un projet cybernétique de pilotage global, de la maison jusqu'à la planète. Là-dessus, La QDN ne dit rien.

(...)

La technopolice, libre ou brevetée, c'est d'abord cela : l'automatisation des entrepôts de La Poste, des pistes de décollage et des avions, des trains et des gares ; le pilotage des voitures autonomes et des boulevards périphériques, des métros et des allées de métro, en vue de leur fluidification ; le puçage des poubelles et des camions-poubelles, des arbres et des jardiniers, sous couvert d'écologie ; la traçabilité des animaux dans leurs élevages automatisés, et jusqu'aux boîtes de conserves auxquelles ils sont destinés. Les compteurs Linky, et leur enregistrement des données, ne sont pas un outil de surveillance machiavélique ou paranoïaque, mais une technologie de pilotage du monde-machine en pleine transition électro-nucléaire - puisque l'usage des outils numériques explose nos besoins en électricité.

La technopolice, la planète intelligente, la smart city, sont d'abord des systèmes de pilotage et de planification de l'économie, en vue de son expansion. Si l'on est écologiste, on combat l'informatisation, et non pas ses « dérives ».

(...)

Quant à la Quadrature du net, elle est à la critique des TIC (technologies de l'information et de la communication), ce que les syndicats sont à la critique de l'économie politique ; des représentants du personnel intéressés à la bonne marche de l'entreprise et débordant de suggestions pour améliorer son fonctionnement. Des geeks et des hackers pourrissant bientôt dans leurs capsules de « réalité virtuelle » et pleurnichant pour que Mark Zuckerberg améliore la qualité immersive de leurs mondes artificiels.

(...)

DIVERS

- **Montélimar : des caméras avec détecteur équipé d'intelligence artificielle anti-dépôts d'ordures sauvages** - Flicage technologique en guise de politique et de vie sociale ?
- **A Putanges-le-lac comme ailleurs, la vidéosurveillance se propage** - Le 25 mai 2022, nos camarades du

collectif Vivre Ensemble Putanges attaquaient l'installation de caméras de vidéosurveillance prévue pour la commune devant le Tribunal administratif de Caen. Cette mobilisation s'inscrit dans le contexte d'un déploiement irréfrénable des caméras de vidéosurveillance partout en France. Elles sont désormais aussi installées dans des villages. Comment déconstruire et lutter contre ce discours pro-caméras et technopolice dominant ?

- **Contrôles discriminatoires : «** Nous demandons le démantèlement des pratiques illégales des CAF » - Contrôles abusifs des allocataires, suspension des versements, harcèlement des plus précaires... La CAF oublie ses missions initiales de protection et de soutien pour devenir un outil de police numérique. Une tribune du collectif « Changer de cap ».
  La numérisation à marche forcée des services publics contribue à faire des Caisses d'allocations familiales (CAF) un instrument de la mise en place d'une société de surveillance et de pénalisation des plus pauvres. Alors que la protection sociale est un droit universel depuis le Conseil national de la Résistance, les CAF développent une politique de plus en plus dure de contrôle des personnes en situation de précarité.
- **Intelligence artificielle : comment les supermarchés, profitant d'un flou juridique, sophistiquent la détection des vols** - Face à la recrudescence des vols dans les magasins, les enseignes testent des solutions qui automatisent leur détection. La CNIL vient d'achever une consultation publique afin de prendre position.
- **Avis aux amateurs : Orange déploie les flics de demain dans ses «** 5G Lab » - Robot autonome de surveillance, télémédecine, vidéosurveillance : Orange teste la 5G dans son « Lab » bordelais (...)
  Car une première précision s'impose : « La 5G, par définition, a été créée pour les usages BtoB ! », rappelle un cadre français de Cradlepoint, filiale d'Ericsson spécialisée dans la fabrication de routeurs 4G et 5G. Cette technologie d'avenir est en effet présentée comme la voie royale pour numériser tous les grands secteurs de l'économie, de l'énergie aux transports, en passant par l'automobile, la banque ou encore la santé. (...)
- **Ils savent tout sur vous et vous ne savez rien sur eux** - Trois milliards de smartphones surveillés en temps réel par une société très discrète. Des révélations choc sur l'espionnage numérique.
- **À Nice, on équipe des caméras de surveillance avec une intelligence artificielle** - La Ville de Nice va expérimenter des caméras équipées d'IA, d'intelligence artificielle. Elles auront la possibilité d'analyser les déplacements urbains de manière beaucoup fine. On ne parle pas de reconnaissance faciale, mais l'analyse va bien au-delà de la simple captation vidéo.
- **«** Ces expérimentations ont pour but d'accoutumer la population à la présence des technologies de surveillance » par Olivier Tesquet - Alors que la commission des lois du Sénat vient d'adopter à l'unanimité un rapport d'information sur la « reconnaissance faciale », le journaliste Olivier Tesquet expose sur QG les dangers d'une telle technologie, et les intentions troubles des sénateurs, qui préconisent une série d'expérimentations sous couvert de protéger les citoyens. Interview par Luc Auffret

Boîte noire dans les voitures

- **Une «** boîte noire » à bord des nouveaux modèles d'automobiles - Enregistreur de données automobiles.
  L'intitulé retenu par les instances européennes est aussi neutre que possible, mais cet équipement, qui fera son apparition à compter du 6 juillet à bord des nouveaux modèles, est d'ores et déjà désigné sous l'appellation de « boîte noire ». Avec les sous-entendus vaguement inquiétants qui accompagnent immanquablement l'introduction de ce genre de dispositif.
  Pas de doute, l'enregistreur, qui deviendra obligatoire dans quelques jours, est bien une « boîte noire ».
  Obligatoire à compter du 6 juillet, cet « enregistreur de données automobiles » ne sera généralisé que dans deux ans.
  (...)
  Le texte, adopté en 2019 par le Parlement européen, précise que ces informations ne seront accessibles qu'aux autorités judiciaires dans le cadre d'une enquête et aux organismes de recherche chargés de dresser des statistiques d'accidentologie.
  (...)
  Reste à savoir si le nouvel enregistreur de données automobiles s'en tiendra à sa fonction initiale consistant à « mener des analyses de sécurité routière et évaluer l'efficacité » des dispositifs existants.

On ne peut exclure que, tôt ou tard, il intéresse, entre autres, les assureurs. Ceux-ci proposent déjà aux Etats-Unis, avec un succès mitigé, une tarification fondée sur le mode de conduite des automobilistes, défini à partir de données stockées par une boîte noire embarquée.
La numérisation des données automobiles, qui permet déjà aux constructeurs de recueillir des quantités de data - anonymisées - ouvre un gigantesque faisceau d'utilisations. En revanche, une diffusion élargie et affinée de ces informations imposerait que le législateur accepte de l'autoriser explicitement.

(ça commence par les accidents, puis la boite noire enregistrera tout en permanence, et les flics pourront y avoir accès pour leurs enquêtes)

L'algorithme et le numérique enferment dans le modèle dominant, "choisi" par le sujet humain

Parcoursup et la police prédictive - La vie, le destin, l'algorithme - Quoi de commun entre la police prédictive et Parcoursup ? Les deux reposent sur des algorithmes, certes, mais ils sont surtout deux outils plus ou moins subtils du contrôle social assisté par ordinateur. À chaque fois, l'algorithme incarne une somme de décisions politiques dont l'importance n'a d'égale que l'opacité : tout repose alors sur l'efficacité opérationelle, l'interface, la baisse du taux de criminalité ou la répartition des élèves dans les filières en fonction de leurs choix. Une fois n'est pas coutume, les causes structurelles ou les déterminations collectives sont converties et neutralisées en décisions individuelles.
(...)
Comme le dit si bien Jean-Michel Blanquer, les élèves sont « ancrés dans leur histoire », en attente, privés de futur. Sans politique, sans démocratie, sans commun, l'ordre marchand et le chaos écologique pour unique horizon.
(...)

Le virtuel et le numérique actualisent une certaine version de la réalité

On peut donc affirmer que Parcoursup est un instrument de police prédictive. Un algorithme public mais dont l'utilisation reste opaque est utilisé pour calculer le parcours des élèves. En fonction des notes, de l'origine sociale et géographique, de la motivation des élèves, de leur C.V., on calcule leur orientation optimale. Le passé est utilisé comme une donnée objective, représenté par des notes, des appréciations, des données, traitées par un algorithme qui produit des classements. Comme avec PredPol, tout ce que vous avez fait dans votre vie est utilisé pour vous empêcher de faire autre chose, tout ce que vous êtes est retenu contre vous. Le futur est vendu avec le passé, et le passé devient linéaire, parcouru sans être vécu. En atomisant et privatisant les individus, ce système prive de la possibilité d'agir collectivement sur le futur.
(...)
L'effet du virtuel et du numérique, c'est donc d'actualiser une certaine version de la réalité, celle qui convient aux classes dominantes de l'heure, tout en frappant d'irréalité les autres possibilités qui existent et persistent malgré tout.
(...) Il est frappant de constater à quel point les technologies de pointe et les discours modernisateurs réactivent des discours réactionnaires anciens. Ceux qui pensent être à la pointe de l'innovation en matière de politique éducative ne font que reprendre certaines des pires tendances des politiques sociales du XXe siècle : la soumission de l'individu à un déterminisme strict, la contingence du social oblitérée derrière des données biologiques ou génétiques présentées comme absolues, un tri social qui prend pour critère l'adaptabilité à l'ordre existant. Tout ceci participe d'un renouveau de l'eugénisme, indexé cette fois-ci non seulement sur une idéologie raciste, mais aussi sur les impératifs de la mondialisation néolibérale (...) *Afin d'offrir à la considération des opprimés et des subjugués un monde de mensonge et de tromperie fabriqué pour accroître leur aliénation et leur passivité, les oppresseurs développent toute une série de méthodes empêchant toute présentation du monde comme problème, en le montrant plutôt comme une entité fixe et établie, quelque chose de donné, quelque chose dont les gens ne sont en fait que de*

simple spectateurs et auquel ils doivent s'adapter.

Le Conseil d'État défend la reconnaissance faciale de masse par la police (qui est d'extrême droite)

Le Conseil d'État sauve la reconnaissance faciale du fichier TAJ - Le 26 avril 2022, le Conseil d'État a rejeté nos critiques contre l'utilisation massive de la reconnaissance faciale par la police dans le TAJ (« traitement des antécédents judiciaires »). Il s'agit d'une défaite cinglante, qui affirme encore davantage le Conseil d'État dans son rôle de défenseur de la surveillance de masse, sans plus aucune considération pour le respect des droits des personnes. Nous avons l'habitude de perdre et de ne pas nous résigner : trouvons dans cette défaite les futures pistes de notre lutte.

(...)

Surtout, et c'était l'objet de notre recours devant le Conseil d'État, le décret TAJ autorise les policiers à utiliser des logiciels de reconnaissance faciale pour consulter sa base de données. **Les policiers peuvent automatiquement comparer une image captée par une caméra de surveillance, un téléphone ou sur Internet aux 8 millions de photographies présentes sur les fiches des personnes mises en cause (chiffres de 2018)**. Cette comparaison a lieu dans le cadre d'enquêtes comme de simples contrôles d'identité, comme l'expliquait le ministre de l'intérieur en 2021.

(...)

le recours à cette technologie est aujourd'hui généralisé. La police a utilisé le TAJ pour faire de la reconnaissance faciale 375 000 fois en 2019, soit plus de 1 000 traitements par jour partout en France

(...)

Présenter le contrôle de la CNIL et des juges comme une garantie suffisante pour pallier ces abus est une échappatoire malhonnête pour permettre le maintien de ces pratiques. C'est le propre de la surveillance de masse que d'échapper à tout encadrement crédible, et c'est cette évidence que le Conseil d'État a niée.

(...)

Une surveillance de masse (le fichage généralisé) rend nécessaire une autre surveillance de masse (la reconnaissance faciale généralisée)

Si le Conseil d'État a refusé de prendre en compte dans sa décision les abus concrets du TAJ, il a quand même cherché à justifier la « nécessité absolue » de la reconnaissance faciale. Sa démonstration est si terrible que nous la restituons telle quelle : « eu égard au nombre de personnes mises en cause enregistrées dans [le TAJ], qui s'élève à plusieurs millions, il est matériellement impossible aux agents compétents de procéder manuellement à une telle comparaison » d'images, dont l'automatisation ne peut dès lors que « s'avérer absolument nécessaire à la recherche des auteurs d'infractions et à la prévention des atteintes à l'ordre public ». **Autrement dit, le recours à des logiciels d'analyse d'images automatisée serait rendu nécessaire car le TAJ, abandonné à la police depuis 10 ans et sans aucun contrôle externe, est devenu si tentaculaire et absurde qu'il ne peut plus être exploité à son plein potentiel par des humains. Une surveillance de masse (le fichage généralisé) rend nécessaire une autre surveillance de masse (la reconnaissance faciale généralisée).**

(...)

En abandonnant son rôle de gardien des libertés, le Conseil d'État valide et inscrit dans le marbre la croyance selon laquelle il faut toujours plus en connaître sur la population, considérée comme étant suspecte par défaut.

(...)

l'Union européenne est en passe d'adopter un règlement sur l'IA qui viendrait légitimer les technologies de surveillances biométriques aujourd'hui interdites par le RGPD (revoir notre analyse) et que la France, actuellement présidente du Conseil de l'UE, fait tout pour défendre son industrie et son idéologie technopolicières.

(...)

NOTE : **Voilà pourquoi les flics filment dorénavant toutes les personnes présentes à n'importe quel rassemblement, à tout événement public (même des concerts ou un simple débat) susceptible d'attirer des contestataires.**

Leçon : les institutions de l'Etat ne peuvent pas nous protéger contre l'Etat. L'Etat de droit et le mantra de "la-démocratie" masquent la réalité d'un système centralisé, autoritaire, policier, oligarchique, mafieux... irréformable.

"Ce que vous êtes en train de créer, c'est l'infrastructure de surveillance biométrique la plus étendue que nous n'ayons jamais vue dans le monde"

En Europe, les plans pour généraliser la reconnaissance faciale avancent.
Ca commence par un bout, en promettant un usage restreint et contrôlé, puis l'usage s'étend à d'autres catégories grâce à des crises opportunes (terrorisme, affaires meurtrières retentissantes, crimes d'enfants...).

Europe Is Building a Huge International Facial Recognition System - Lawmakers advance proposals to let police forces across the EU link their photo databasesâ€"which include millions of pictures of people's faces.
(traduction : **L'Europe met en place un gigantesque système international de reconnaissance faciale**
Les législateurs avancent des propositions visant à permettre aux forces de police de l'Union européenne de relier leurs bases de données photographiques, qui contiennent des millions de photos de visages.

Extraits traduits (de manière approximative) :
(...)
Depuis 15 ans, les forces de police qui recherchent des criminels en Europe peuvent échanger leurs empreintes digitales, leurs données ADN et des informations sur les propriétaires de véhicules. Si des fonctionnaires français soupçonnent qu'une personne qu'ils recherchent se trouve en Espagne, ils peuvent demander aux autorités espagnoles de vérifier les empreintes digitales dans leur base de données. Aujourd'hui, les législateurs européens s'apprêtent à inclure des millions de photos de visages dans ce système et à permettre l'utilisation de la reconnaissance faciale à une échelle sans précédent.
(...)
Prüm II prévoit d'élargir considérablement la quantité d'informations pouvant être partagées, en incluant potentiellement des photos et des informations provenant des permis de conduire. Les propositions de la Commission européenne prévoient également que la police disposera d'un accès "automatisé" plus large aux informations partagées. Selon les législateurs, cela signifie que les polices de toute l'Europe pourront coopérer étroitement et que l'agence européenne de police Europol aura un "rôle plus important".

L'inclusion d'images faciales et la possibilité d'exécuter des algorithmes de reconnaissance faciale sur ces images figurent parmi les principaux changements prévus dans Prüm II. Ces dernières années, la technologie de la reconnaissance faciale a fait l'objet d'importantes critiques de la part des forces de police, qui l'ont de plus en plus adoptée. Des dizaines de villes américaines sont allées jusqu'à interdire aux forces de police d'utiliser cette technologie. L'Union européenne débat actuellement d'une interdiction de l'utilisation par la police de la reconnaissance faciale dans les lieux publics dans le cadre de sa loi sur l'intelligence artificielle.

Toutefois, la loi Prüm II autorise l'utilisation de la reconnaissance faciale rétrospective. **Cela signifie que les forces de police peuvent comparer les images fixes des caméras de vidéosurveillance, les photos des médias sociaux ou celles du téléphone d'une victime avec les photos d'identité judiciaire conservées dans une base de données de la police. Cette technologie est différente des systèmes de reconnaissance faciale en direct,**

qui sont souvent connectés à des caméras dans des espaces publics ; ce sont ces derniers qui ont été les plus critiqués.

(...)

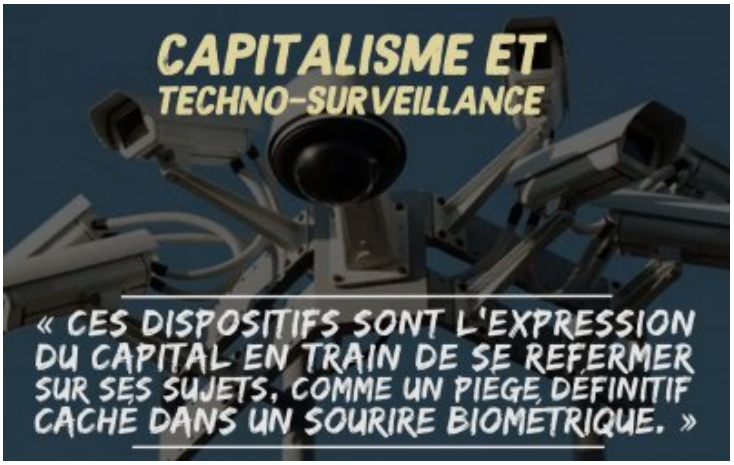
La Hongrie possède 30 millions de photos, l'Italie 17 millions, la France 6 millions et l'Allemagne 5,5 millions, indiquent les documents. Ces images peuvent inclure des suspects, des personnes condamnées pour des crimes, des demandeurs d'asile et des "cadavres non identifiés", et elles proviennent de sources multiples dans chaque pays.

Selon Mme Jakubowska, si les critiques à l'encontre des systèmes de reconnaissance faciale ont surtout porté sur les systèmes en temps réel, ceux qui identifient les personnes à une date ultérieure restent problématiques. "Lorsque vous appliquez la reconnaissance faciale à des séquences ou à des images de manière rétrospective, les préjudices peuvent parfois être encore plus importants, en raison de la capacité à regarder en arrière, disons, une manifestation d'il y a trois ans, ou à voir qui j'ai rencontré il y a cinq ans, parce que je suis maintenant un adversaire politique", dit-elle. "Seules les images faciales de suspects ou de criminels condamnés peuvent être échangées", précise le porte-parole de la Commission européenne, citant un guide sur le fonctionnement du système. "Il n'y aura pas de correspondance entre les images faciales et celles de la population générale".

(...)

"La recherche automatisée d'images faciales n'est pas limitée uniquement aux crimes graves, mais pourrait être effectuée pour la prévention, la détection et l'enquête de toute infraction pénale, même mineure", a déclaré Wojciech Wiewiórowski, le CEPD, début mars. Wiewiórowski a déclaré que plus de garanties devraient être écrites dans les propositions pour s'assurer que les droits à la vie privée des personnes sont protégés. Le porte-parole de la Commission européenne a déclaré que l'organisme a pris "bonne note" de l'avis du CEPD et que les réflexions seront prises en compte lorsque le Parlement européen et le Conseil discuteront de la législation.

(...)



La technopolice c'est la ville connectée, la smart city : chronique de la numérisation de la gestion du monde

Techno-surveillance totale pour Â« citoyen Â» monitorés H24 : c'est ça le progrès

A CAPITALISME ET TECHNO-SURVEILLANCE

« Ces dispositifs sont l'expression du capital en train de se refermer sur ses sujets, comme un piège définitif caché dans un sourire biométrique » Sandrine Aumercier

Alors qu'on punit déjà plus sévèrement un jeune homme pour le vol d'un sandwich que les propriétaires du capital responsables de tragédies partout sur le globe, que des millions de personnes sont persécutées parce qu'elles tentent de fuir ces mêmes tragédies ou encore que certains pachas de plateaux télé appellent à qualifier de terrorisme un colère légitime contre une vitrine des instruments financiers rendant tout cela possible, le capitalisme dans son stade agonisant invente encore de nouveaux outils de contrôle des populations.

Bienvenue dans le monde des algorithmes, de la « vidéo surveillance intelligente » et du crédit citoyen. La Méditerranée est devenue un cimetière, de l'autre côté de la rive on a vu des marchés aux esclaves, des îles sont transformées en prison et le traitement des demandes d'asile est externalisé auprès de dictatures mais l'Union Européenne ne s'en soucie guère, ce qui compte c'est la préservation d'une forteresse qui ne fait que s'accaparer les richesses d'un monde extérieur dont elle continue de dégrader les conditions d'existence.

Dans cette logique, depuis 2016, la commission Européenne met au point le dispositif iBorderCtrl (renommé depuis iCROSS) dont aucun média à la solde du système n'a parlé. De janvier à août 2019, une première expérimentation a été mise en place sur les frontières grecques, hongroises et lettonnes. Cette technologie dite de « contrôle intelligent », qui a coûté plus de quatre millions d'euro, se donne pour objectif de fluidifier le passage aux frontières tout en faisant face à « la menace croissante d'immigration illégale ».

La procédure consiste à soumettre son passage à la frontière à l'interaction avec un machine qui analyse les documents fournis, pratique la reconnaissance faciale, pose des questions « personnalisées » et détecte les mensonges, après quoi les individus sont aiguillé vers une file à « bas risque » et une autre à « haut risque ». Sans parler du taux d'échec de ces algorithmes de plus de 25%, ce processus complètement inhumain n'est qu'un pas de plus vers une société où la surveillance adossée à des machines prends le pas sur nos vies.

Des ordinateurs détectent des actions anormales de la part des citoyen-ne-s.

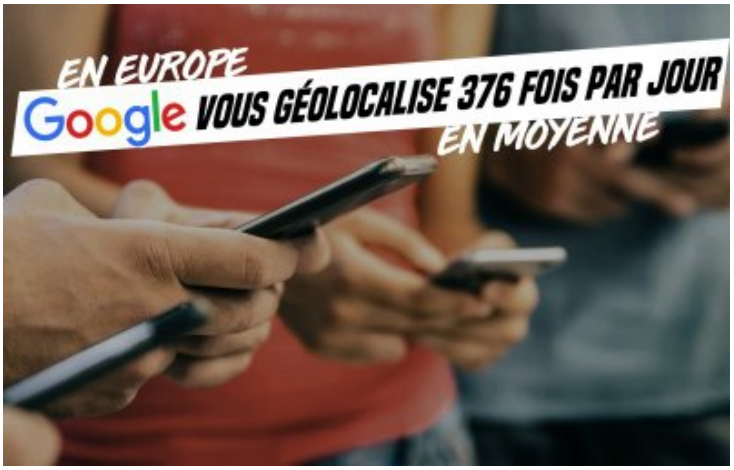
Autre exemple de cette délégation aux « IA » : la vidéosurveillance 2.0. À force de mettre des caméras partout les organes de contrôles manquent d'humains pour analyser les flux d'images, leur solution est donc de confier leur traitement à des algorithmes. Des sociétés, comme le groupe français XXII, se spécialisent dans des solutions qui confient à des ordinateurs la détection des actions anormales de la part des citoyen-ne-s. La ville de Suresnes (92) a ainsi conclu un contrat avec XXII afin de coupler le logiciel à leur réseau de caméra dans le but d'identifier les maraudages ou les rassemblements de personnes. Mais cela ne s'arrête pas là, une entreprise de Metz a développé un logiciel d'« hypervision » qui permet d'afficher sur une carte le non respect du port du masque, de la distanciation sociale ou encore les cas de fièvre.

Malgré l'absence de texte de loi autorisant ces technologies, le plus souvent les entreprises les implémentent pour leur clients sous couvert d'expérimentation. Si ces systèmes externes de contrôle des populations sont inquiétants, ceux que les gens seront d'accord de porter eux-mêmes le sont davantage.

En Italie, un « portefeuille numérique du citoyen vertueux »

En Italie, la ville de Bologne va bientôt lancer un « portefeuille du citoyen vertueux ». Ce portefeuille fonctionnera ainsi : « Les citoyens seront reconnus s'ils trient les déchets, s'ils utilisent les transports en commun, s'ils gèrent bien l'énergie, s'ils ne prennent pas de sanctions de la part de l'autorité municipale, s'ils sont actifs avec la carte culture ». Les points ainsi cumulés pourront être convertis en lots dont la nature n'est pas encore précisée. Ce système poussera les plus précaires à l'adopter en vue d'accroître légèrement leur pouvoir d'achat, il faut bien un peu d'incitation car pour l'instant il ne s'agit encore que de volontariat et là aussi sur des bases expérimentales, c'est fou ce que les tenant de la techno-surveillance adorent l'expérimentation !

Si, pour l'instant, le système fonctionne au bonus, ne soyons pas dupes : les malus arriveront un jour. Travail, consomme et ferme ta gueule, le tout sous le contrôle des algorithmes, voilà l'avenir du capitalisme de techno-surveillance.



La technopolice c'est la ville connectée, la smart city : chronique de la numérisation de la gestion du monde
Les multinationales vous pistent H24 partout

EN EUROPE, GOOGLE VOUS GÉOLOCALISE 376 FOIS PAR JOUR EN MOYENNE

En Irlande, le Conseil pour les libertés civiles - ICCL - a réalisé une enquête sur l'ampleur du phénomène numérique appelé RTB, soit real-time bidding ou « offre en temps réel » en français. Ce procédé consiste, pour Google et les autres grands acteurs tech, à nous géolocaliser presque en permanence. Particulièrement en cause, le RTB qui est un type de publicité reposant sur la mise aux enchères d'un espace de diffusion. L'enquête se base sur des chiffres publics, mais aussi certaines sources confidentielles.

Concrètement, lorsqu'un utilisateur consulte une page web avec un encart publicitaire, son profil est automatiquement analysé par différents annonceurs potentiels, qui ont alors accès à plusieurs informations le concernant, et notamment sa géolocalisation. En croisant un certain nombre de données, les entreprises se livrent alors à une vente aux enchères, qui déterminera par la suite quelle publicité afficher en fonction du profil utilisateur et du prix mis sur la table. Cette opération ne prend qu'une fraction de seconde.

Google partagerait ainsi 71 milliards de géolocalisations RTB en Europe chaque année. Un Européen est donc géolocalisé en moyenne 376 fois par jour. Et ce chiffre est de moitié inférieur à celui enregistré aux États-Unis, où aucun règlement ne garantit la sécurité des données en ligne. Selon l'ICCL, ces résultats sont d'autant plus inquiétants qu'ils pourraient être très en dessous du nombre réel. Les chiffres du rapport indiquent en effet qu'il s'agit là d'une « estimation basse », qui n'inclut pas les diffusions RTB de Facebook ou Amazon. **Ni la géolocalisation qui peut être organisée par les institutions de surveillance étatiques...**

(posts de Nantes Révoltée)

@ ESSAIM DE DRONES AUTONOMES : FUTUR CAUCHEMAR DE LA TECHNO-POLICE ? @

C'est une première mondiale : il y a deux semaines, des scientifiques de l'Université chinoise de Zheijiang publiaient une vidéo pour le moins inquiétante d'un essaim de dix drônes capables de s'adapter à leur environnement en temps réel, dans une forêt sans être guidés par des êtres humains.

Équipés d'un ordinateur, d'un capteur, d'une caméra et d'un algorithme spécifiquement étudié pour chacun d'entre eux, ces drônes arrivent à se repérer sans ordinateur central en gardant une distance de sécurité. Ils cartographient une trajectoire planifiée seuls.

Tous les obstacles dans la forêt dans laquelle ils naviguent sont esquivés minutieusement.

Après les drônes, les robots-tueurs ou les chiens robots, le monde d'Orwell apparaît presque comme raisonnable

Le média Numérama rapporte que : "Les drônes étaient bardés de capteurs afin de traiter individuellement, et de partager en temps réel, les données qu'ils collectaient aux autres drônes.
Ils embarquaient par exemple des caméras et des capteurs d'altitude pour évaluer leur propre position. Ainsi, grâce à un algorithme embarqué dans chacun d'eux, les petits avions sans pilotes parviennent à maintenir une certaine distance de sécurité entre eux pour éviter toute collision avec les arbres ou d'autres drones."

Difficile d'imaginer comment cette expérience ne contribuera pas d'un côté à une utilisation militaire et répressive, même si elle pourrait aussi être utilisée durant des catastrophes naturelles, capables de se repérer sans GPS.

Après les drônes, les robots-tueurs ou plus récemment les chiens robots, le monde d'Orwell apparaît presque comme raisonnable si on le compare à notre futur proche.

- Vidéo : https://fb.watch/d57IrlKmPD/

(post de Cerveaux non disponibles)

- Voir aussi :
- **Cet essaim de drones est autonome en énergie et vous suivra partout** - Des chercheurs ont imaginé un « Internet des drones » capable de produire sa propre énergie sans intervention humaine. Une idée proprement terrifiante.

La technopolice c'est la ville connectée, la smart city : chronique de la numérisation de la gestion du monde
Pour le capitalisme, tout ce qui peut être rentable doit être marchandisé

VERS UN MARCHÉ DES DONNÉES DE SANTÉ ?

Des nouvelles de l'industrie techno-sanitaire

Au début du mois la commission européenne a exposé sa proposition pour l'instauration d'une nouvelle modalité de gestion des données numériques en matière de santé : l'espace européen des données de santé. Après l'épidémie de Covid et toutes les controverses au sujet du contrôle numérique sanitaire, certains points de cette nouvelle réglementation peuvent nous inquiéter.

Les informations relatives à la santé sont particulièrement sensibles, elles touchent à ce qu'il y a des plus intime chez les personnes. Les objectifs annoncés sont de favoriser l'accès, pour les individus, à un certain nombre de leurs informations médicales, d'harmoniser cet accès au niveau européen et de permettre de développer la recherche scientifique. **Mais il est également stipulé que ce dispositif permettra le développement de nouveaux services et produit de santé numérique. Le marché trouvera alors toute une série de nouveaux débouchés : dossiers médicaux électroniques, logiciels médicaux ou encore applications de « bien-être ». C'est là que les problèmes commencent. Rien ne nous garantit que la concentration de ces informations numériques par les pouvoirs publics, mais aussi par les industriels, ne se fera pas au détriment de nos droits et libertés.**

Le marché des données de santé, nouveau filon juteux pour le capitalisme avide de tout secteur à transformer en argent

Parmi les services nouveaux que la réglementation doit permettre figure la téléconsultation. Un pas de plus dans la libéralisation du marché de la santé, mais aussi dans sa délocalisation. Avec ces dispositifs il sera possible de voir sa consultation à distance effectuée très à distance, à l'autre bout de l'UE par exemple.
Les applications de mesure des données physiologiques sont, elles aussi, une porte ouverte à un nouveau marché que les industriels aimeraient bien voir remboursé par la sécurité sociale. Les montres connectées et autre appareils dotés de capteurs permettant l'auto-diagnostic risquent de mettre en place un système de télésurveillance. **Les géants du numérique se frottent doublement les mains : ils pourront à la fois fournir les service d'hébergement des données et bénéficier de l'usage de ces dernières. De plus, on ouvre la porte à ce que ces données finissent chez les assureurs qui pourront ainsi « adapter » leurs primes aux comportements des individus**, même si pour l'instant ce type d'utilisation et expressément exclu Dans l'UE. Mais avec le concentration d'un grand nombre de données sensibles l'effet « pot de miel » est fort, les risques de failles ne sont pas à négliger et les tentatives de hacking non plus.

Enfin rappelons que les risques en matière de données médicales sont encore plus grands pour les personnes exposées aux discriminations. En fin d'année dernière, des collectif de défense des droits des personnes trans ou luttant contre la psychophobie avaient alertés sur les danger du dispositif « mon espace santé » sur Ameli. Ce dernier ne cloisonnait pas correctement les informations et exposait les personnes à des outings non désirés, ou encore à des traitements discriminatoires par le corps médical.

Nos données nous appartiennent, elles ne doivent pas faire l'objet d'un marché ou d'une surveillance toujours plus accrue de nos faits et gestes !

(post de Nantes Révoltée)

Copyright © Ricochets