https://ricochets.cc/Chronique-technopolice-surveillance-preventive-et-predictive-canon-a-son-pass-sanitaire-drones-armes-identification-visage-logiciel-espion.html

Chronique de la technopolice : surveillance préventive et prédictive, canon à son, pass sanitaire informatisé, drones armés, identification des visages, logiciel espion...

Publication date: samedi 24 juillet 2021

- Les Articles -

Reconnaissance faciale et logiciels d'analyse comportementale dans les gares et train de Rhône-alpes !

Lundi, Laurent Wauquiez veut autoriser la reconnaissance faciale dans les trains et les gares - Lundi 19 juillet prochain, Laurent Wauquiez présentera à l'assemblée de la région Auvergne-Rhône-Alpes un projet de délibération pour lui permettre de déployer la reconnaissance faciale dans les gares, de financer l'achat de logiciel d'analyses comportementales et de multiplier les caméras de vidéosurveillance. C'est un pur projet de Technopolice, dangereux et illégal, que l'assemblée plénière du conseil régional se doit de rejeter.

Il est probable que Laurent Wauquiez et son équipe soient parfaitement conscients de l'illégalité de leur projet. On imagine que, comme Valérie Pécresse ou Christian Estrosi, la véracité de leur propos ou la légalité de leurs actions ne les intéressent que peu. Ils veulent avant tout mettre en avant une idéologie sécuritaire, qu'ils imaginent flatter une certaine catégorie d'électeurs en vue des échéances électorales à venir. A chaque échéance, ils iront donc un peu plus loin dans leurs propositions.

Il faut que cessent ces projets mis en place illégalement par la classe politique, comme l'usage de drones par la police l'année dernière et tous ces projets technopoliciers que nous avons pu participer à faire échouer. Il faut leur opposer, aujourd'hui et demain, notre refus de la surveillance biométrique et du tout-sécuritaire. Il nous faut dénoncer leurs fantasmes totalitaires. Nous appelons le conseil régional à s'opposer lundi prochain à ce projet de délibération.

Chronique de la technopolice : surveillance préventive et prédictive, canon à son, pass sanitaire informatisé, drones armés, identification des visages, logiciel espion... Des logiciels perfectionnés pour aspirer toutes vos données et surveiller

Tous les français placés sous surveillance algorithmique préventive et prédictive

Anti-terrorisme ? Nouvelle loi renseignement : le gouvernement place la population sous surveillance algorithmique - Conservation généralisée des données de connexion, surveillance de masse... Adopté par les députés, avant le Sénat fin juin, le projet de loi renseignement passe en procédure accélérée. Mais son contenu inquiétant mériterait un débat public d'ampleur.

(...)

Dans tous les cas, il est désormais officiel que les algorithmes de surveillance seront étendus aux URL.

(...)

Résumons : les services de renseignement mettent en place diverses techniques d'interception de données - écoutes téléphoniques, puces GPS aposées sur les véhicules, captation des données de smartphones... Désormais,

ces données brutes seront transmises à une équipe centralisée pour en faire de la recherche et développement, ou « R&D ». De quoi s'agit-il ? De « machine-learning » : ce stock de données sera exploité pour approfondir les outils techniques du renseignement comme améliorer la transcription de voix, faire de la recherche prédictive (par exemple, parvenir à prévoir le parcours d'une personne), etc.

« Un monstre qui grandit dans l'ombre » : voilà ce que constitue, pour Arthur Messaud, cette nouveauté. « Un État qui conserve pendant cinq ans les données captées de la population... Il y a deux ans, ça aurait fait la Une de la presse pendant des semaines » se désespère le juriste. Pour lui, il s'agit d'un copié-collé du modèle de recherche exploratoire de la NSA, révélé par Edward Snowden. Ou de la logique de sociétés privées spécialisées sur la R&D, comme Palantir. Cette entreprise - qui porte le nom d'un objet légendaire du Seigneur des Anneaux permettant d'observer des scènes éloignées dans le temps et l'espace - fournit, depuis 2015, des technologies de traitement de la donnée aux renseignements français.

« Et si le gouvernement suivant produit des lois permettant d'aller piocher dans ces stocks de données pour d'autres finalités que la R&D ? », interroge Pierre, du CECIL. Ces informations pourraient alors servir d'autres objectifs : surveillance économique, répression des opposants politiques... « Les lois sécuritaires reposent presque systématiquement sur ces tours de passe-passe à deux étapes » s'inquiète à ce sujet la Quadrature du Net.
(...)
Le 28 avril, Gérald Darmanin, ministre de l'Intérieur, avait fait une déclaration fracassante sur France Inter, affirmant : « Nous discutons avec les grands majors d'Internet, on leur demande de nous laisser entrer via des failles de sécurité » pour contourner le chiffrement des communications. Le « piratage » d'un téléphone ou d'une box internet par des services de renseignement n'est pas nouveau. Mais cette fois, avec l'article 10 du projet de loi, « la nouveauté, c'est que les opérateurs vont devoir coopérer avec les services » explique Arthur Messaud.

Ces opérateurs sont les entreprises qui fournissent votre service internet, gèrent le réseau, ou proposent des outils de communication interpersonnelle : Gmail, Zoom, WhatsApp, Signal, Telegram... Les services de renseignement pourront désormais leur demander de compromettre leurs dispositifs techniques - pour « hacker » votre box par exemple. Jusqu'ici, rien ne les y obligeait légalement.
(...)

Nos commentaires sur **Le gouvernement français veut placer toute la population sous surveillance algorithmique**

Lecture
LOI RENSEIGNEMENT : LE GOUVERNEMENT NOUS MET TOUS SOUS SURVEILLANCE par [BLAST - Le souffle de l'info-Â»https://www.youtube.com/c/Blast-info]
https://www.youtube.com/watch?v=KxtF33v5beI

Le Sénat a adopté, le mercredi 30 juin, un projet de loi renforçant les mesures antiterroristes et le renseignement. Voté par 251 voix contre 27 et 66 abstentions, le texte, dont les sénateurs ont modifié plusieurs articles, pérennise des mesures inspirées de l'état d'urgence.

Annoncé dans la foulée de l'attentat contre une fonctionnaire de police à Rambouillet en avril, ce nouveau projet de loi dans l'arsenal antiterroriste était programmé de longue date. Il vise notamment à faire entrer définitivement dans le droit commun quatre mesures emblématiques mais expérimentales de la loi « sécurité intérieure et lutte contre le terrorisme » (Silt) de 2017.

Conservation généralisée des données de connexion, recours aux algorithmes pour traités ces mêmes données, surveillance de masse, certaines de ces mesures inquiètent et cristallisent de nombreuses oppositions.

Pour en parler Blast reçoit Anne Sophie Simpere, Chargée de plaidoyer Libertés à Amnesty International France et Ugo Bernalicis, député LFI du Nord.

En Auvergne-Rhône-Alpes, surveillance biométrique avec reconnaissance faciale en vue

En Auvergne-Rhône-Alpes, Laurent Wauquiez veut dans son programme accentuer la vidéosurveillance partout, y compris biométrique :

- Brigade de sécurité dans les lycées et leurs abords
- Augmentation de 50% des effectifs de la police ferroviaire
- **10 000 nouvelles caméras de vidéosurveillance**
- **Expérimentation de la reconnaissance faciale** pour lutter contre le terrorisme
- **Bus scolaires équipés en caméras de vidéosurveillance**

Un rapport d'information prospectif au Sénat de juin 2021, qui plaide pour un contrôle numérique très très étendu

Contrainte numérique : des sénateurs lâchent le morceau - Il ne s'agit pas d'un complot, mais d'un rapport sénatorial. De ces intenses cogitations à huis-clos qui tôt ou tard se transforment en lois et changent nos vies.
Les auteurs : Véronique Guillotin, médecin et sénatrice de Meurthe-et-Moselle (Mouvement radical), Christine Lavarde, ingénieur et sénatrice des Hauts-de-France (Les Républicains), René-Paul Savary, médecin et sénateur de la Marne (Les Républicains).
Le titre de ce rapport du 3 juin 2021 : "Sur les crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés".

Vous n'avez jamais rêvé d'être une petite souris dans les réunions internes des puissants, pour entendre ce qu'ils disent de nous et de leurs projets ? Ou bien d'avoir un logiciel espion Pegasus, puisqu'il paraît que "la technologie est neutre et tout dépend ce qu'on en fait" ? Voici un autre moyen, encore plus simple : lire les rapports parlementaires.
Celui-ci est terrifiant (mais on ne les lit pas tous), tant il exhibe de morgue véhémente chez nos biocrates et d'aspiration crue à la technocrature.
On résume : la crise étant le prétexte, saisissons l'occasion pour accélérer et renforcer des mutations en cours. De l'art pour la technocratie d'utiliser la pandémie pour forcer la voie à ses projets de rationalisation et de machination du monde.

Bracelet électronique, contrôle des opérations bancaires, des fréquentations, hausse des cotisations sociales, amendes automatiques, le contrôle de l'état de santé via des objets connectés, alertes automatisées, caméras thermiques dans les restaurants, etc.

- Sommaire du rapport : Crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés
- Résumé en PDF
- Un extrait révélateur sur les visées de contrôle numérique généralisée :

Les rapporteurs (LR et centre) : Véronique GUILLOTIN (a bossé dans un groupe de santé, Christine LAVARDE (a bossé dans la banque Société générale, pour du trading algorithmique), du boursicotage automatisé), René-Paul SAVARY sont à fond pour le contrôle numérique des populations par l'Etat.
Ils mettent habilement en balance le recours à des technologies plus intrusives et les confinements, avec centralisation des données, fichage, contraintes policières..., comme si d'autres solutions n'étaient pas possibles, et surtout en évitant soigneusement la question de couper court à ce qui cause et aggrave les pandémies.

Chronique de la technopolice : surveillance préventive et prédictive, canon à son, pass sanitaire informatisé, drones armés, identification des visages, logiciel espion... Transparence de la foule pour réprimer à l'avance tout comportement potentiellement en voie de subversion

Canon à son pour évacuer les jeunes rassemblés aux Invalides. Une nouveauté en France

Hier à Paris, la police a utilisé (en plus des charges et lacrymo) un canon à son pour évacuer les jeunes rassemblés aux Invalides. C'est une nouveauté en France. Aux Usa, la justice a condamné la police de NY à verser des indemnités à des manifestants aux oreilles abîmées par ces LRAD (long range acoustic device), qui peuvent atteindre 150 db.

Images Yazid Bouziar

(post et vidéo de Cerveaux non disponibles)

Vaccination obligatoire avec pass sanitaire informatisé

« Je suis vacciné mais je suis contre la traçabilité totalitaire qu'ils sont en train de mettre en place, j'ai vécu 5 ans en Chine je suis sûr que c'est une atteinte aux libertés. »

- https://www.facebook.com/watch/?v=508562650218892

Chronique de la technopolice : surveillance préventive et prédictive, canon à son, pass sanitaire informatisé, drones armés, identification des visages, logiciel espion... Armes futuristes d'aujourd'hui

CONTRER LES ARMES DE L'ÉTAT

La dernière nouveauté du ministère de l'intérieur est l'utilisation d'une arme de nouvelle génération qui consiste à envoyer des ondes longues fréquences afin de causer des dommages intra-corporel aux manifestants.
Le but est de faire mal au tympan en utilisant des canon a son afin de faire reculer la foule.

Cette pratique provient des USA qui ont été obligés des versé des indemnités aux victimes de cette arme qui est aujourd'hui interdite dans le cadre des manifestations aux USA.
Pour les contrer rien de plus simple que d'acheter des bouchons d'oreilles disponible en grande surface, pharmacie ou magasin de bricolage.
Il est important de rappeler que l'anatomie humaine est constitué au niveau de l'ouïe de plusieurs "cils" qui permettent de traduire des mouvement d'onde dans l'air en signaux électriques pouvant être déchiffrer par le cerveau.
Les cils au fur et mesure du temps deviennent de moins en moins nombreux et diminue la capacité sonore où pire peuvent provoquer dans les cas les plus extrême des acouphènes isolé ou permanent.

Cette arme ce contre facilement en manif, donc maintenant venez avec des protections auditives

(post de Partage Info Medic et Violences policières)

Divers

- **Épidémie de surveillance : cas pratiques : Olivier Tesquet : «** Dans la rue comme sur Facebook, notre visage ne nous appartient plus » - État d'urgence technologique. Voilà le titre aussi parlant qu'alarmant du dernier ouvrage du journaliste Olivier Tesquet. Il y décrit comment la surveillance généralisée a étendu son emprise à la faveur de la pandémie, avec d'étranges acteurs aux manettes. Zoom, en sa compagnie, sur cinq entreprises méconnues du grand public qui propagent le germe du flicage technologique à vitesse grand V(irus).
- « Le Bureau des légendes », pourvoyeur de recrues pour le renseignement français - « Vocations en séries » (1/6). Ingénieurs, analystes, linguistes... Depuis 2018, les métiers du renseignement attirent de plus en plus les

jeunes, grâce au succès de la série de Canal+, sur lequel la DGSE n'hésite pas à s'appuyer.

- **Comment le gouvernement impose le fichage biométrique aux enfants étrangers isolés** - La préfecture deviendra-t-elle la porte d'entrée de la protection de l'enfance pour les jeunes exilés ? Certains départements refusaient encore de recourir au controversé fichier biométrique. Mais deux projets de loi prévoient sa généralisation.

Des drones armés en essaim font la guerre, ...en attendant les robots tueurs autonomes

Guerre des drones : la menace des essaims - Les récents conflits en Ukraine, en Syrie, en Libye et en particulier dans le Haut-Karabakh ont vu l'utilisation inédite et massive de salves de drones armés. Combinées aux moyens militaires classiques, elles ont des effets dévastateurs pour les troupes au sol.
(...)
En parallèle à cette course aux armements, qui laisse augurer une augmentation en nombre, en intensité et en autonomie des salves de drones, le débat éthique s'avère paradoxalement limité. Après avoir été vif dans les Etats-Unis de Barack Obama (2009-2017), en raison de l'emploi massif de drones pour des assassinats ciblés, il soulève la polémique au sein de la classe politique allemande, mais n'est porté, aujourd'hui dans le reste de l'Europe, que par quelques défenseurs des droits humains. Dans les instances internationales, il s'incarne dans un rapport annuel des Nations unies sur les exécutions extrajudiciaires, sommaires ou arbitraires.

Les salves de drones sont en fait à la croisée d'un autre débat, aux contours techniques encore plus épineux : les systèmes d'armes létales autonomes (SALA), parfois résumés par l'expression « robots tueurs ». Des discussions ont démarré, en 2014, dans le cadre onusien de la Convention sur certaines armes classiques. Depuis, un groupe d'experts se réunit chaque année, « mais, à la question "faut-il interdire préventivement les SALA ? ", aucun consensus entre Etats ne s'est dégagé », souligne M. Jeangène Vilmer, et les négociations piétinent.

Elles butent en particulier sur les secrets technologiques entourant la fabrication d'armes autonomes. Si le contrôle de la prolifération des armements classiques tient de la prouesse, celui des drones plus ou moins autonomes relèvera d'un défi encore plus complexe, prévient le directeur de l'Irsem. L'enjeu technologique des salves de drones ne concerne pas tant les appareils en tant que tels, que les lignes de codes informatiques permettant de les coordonner. Cela explique la volonté, côté français par exemple, de plaider pour un code de bonne conduite qui fixerait une pression normative, plutôt que pour une franche interdiction.

Chronique de la technopolice : surveillance préventive et prédictive, canon à son, pass sanitaire informatisé, drones armés, identification des visages, logiciel espion... Traiter les humains comme des objets mesurables producteurs de données à mettre dans les bons flux

Surveillance et reconnaissance faciale

22 AnyVision - une startup israélienne qui a construit des techniques basées sur l'intelligence artificielle pour identifier les gens par leur visage, mais aussi des technologies liées telles que des contrôles de température pour détecter des températures plus élevées dans une foule - a récolté 235 millions de dollars en financement.

Ses systèmes sont utilisés dans la vidéo-surveillance, les alertes sur la liste de surveillance et les scénarios dans lesquels une organisation cherche à surveiller les foules et à les contrôler...
La startup a fait l'objet d'un rapport en 2019 selon lequel le gouvernement israélien utilisait sa technologie pour surveiller les Palestiniens en Cisjordanie.
L ' entreprise a refusé, mais l'histoire s'est rapidement transformée en une énorme tâche sur sa réputation...
Cela a conduit Microsoft, qui avait investi dans AnyVision, à effectuer un audit complet de l'investissement et de sa position sur les investissements de reconnaissance faciale dans l'ensemble. En fin de compte, Microsoft a cédé sa participation et s'est engagé à ne pas investir dans d'autres technologies comme celle-ci.

Un rapport de Reuters en avril de cette année a montré combien de compagnies utilisent la technologie d'AnyVision aujourd'hui, allant d'hôpitaux comme Cedars Sinai à Los Angeles à des grands détaillants comme Macy ' s et le géant énergétique BP. Les connexions d'AnyVision au pouvoir vont au-delà du simple fait d'avoir de grands clients : il s'avère également que le secrétaire de presse de la Maison Blanche, Jen Psaki, a une fois servi de consultant en communication pour la
Ensuite, un rapport publié hier dans The Markup, a été peigné à travers divers dossiers publics pour AnyVision, y compris un guide d'utilisation de 2019, qui a également permis de peindre un aperçu assez accablant de la quantité d'informations que peut recueillir l'entreprise et de En train de travailler. (Un pilote, et un rapport qui en résulte, impliquait le suivi des enfants dans un district scolaire au Texas : AnyVision a collecté 5,000 photos d'étudiants et a effectué plus de 164,000 détections en seulement sept jours.) 22

source :
https://techcrunch.com/2021/07/07/anyvision-the-controversial-facial-recognition-startup-has-raised-235m-led-by-softbank-and-eldridge/

"PEGASUS" : UN LOGICIEL ESPION ISRAÉLIEN UTILISÉ PAR LES ÉTATS POUR TRAQUER JOURNALISTES ET OPPOSANTS

- **L'outil peut aspirer toutes les données d'un téléphone, y compris les conversations chiffrées** -

Pégase est le cheval ailé de la mythologie grecque, symbole de la créativité. Dans le monde actuel, le nom de cette créature fantastique est récupéré par une firme israélienne pour espionner la vie de dizaines de milliers de personnes.
L'entreprise NSO emploie 750 salarié-es et a mis au point un logiciel espion, Pegasus, utilisé par de nombreux gouvernements dans le monde pour espionner leurs propres populations, ou des citoyens étrangers qui dérangent leurs affaires. Officiellement Pegasus a pour but d'aider les services de renseignement à lutter contre la criminalité, la firme prétend qu'elle « crée des technologies qui aident les agences gouvernementales à prévenir et à enquêter sur le terrorisme et les crimes, pour sauver des milliers de vie dans le monde ». En réalité le logiciel est utilisé en dehors de tout cadre légal et le « terrorisme et grand banditisme » ne constituent qu'une infime partie des utilisations.

Concrètement, Pegasus profite des failles dans les systèmes d'exploitation des smartphones et permet d'avoir accès à toutes les données : photos, numéros et adresses, lire les emails, suivre les conversations, même sur les messageries chiffrées, géolocaliser l'appareil et activer micros et caméras discrètement,

permettant de filmer et d'enregistrer une personne à son insu. Beaucoup plus invasif que l'écoute téléphonique ou la géolocalisation. Plus de 50000 personnes ont été espionnées, dont 1000 français-es et 180 journalistes, ainsi que des athlètes, des prêtres et des imams, des journalistes, des youtubeur-ses, des avocat-es, des syndicalistes... Ou encore des hommes et des femmes dont le seul tort est d'être proches, par liens d'amitié ou familial, de personnes critiques du gouvernement.

Au Mexique, près de 15000 numéros sont des « cibles » de Pegasus. Parmi eux, un journaliste assassiné en 2017, Cecilio Pineda, quelques semaines après que son numéro soit apparu dans le listing. En Arabie Saoudite, le logiciel est utilisé juste avant que le prince héritier n'entame une purge parmi près de 500 de ses opposant-es. En Hongrie, les numéros de dix avocats ont été rentrés dans le système Pegasus. En France, ce sont des journalistes de Médiapart, du Monde, du Canard Enchainé ou de l'Humanité. Surveillance de la presse, assassinats, traque des opposant-es, à l'aide de technologies de pointe.

Et si le logiciel au cheval ailé est découvert, d'autres outils du même type sont très probablement utilisés, tout aussi secrètement et illégalement, par d'autres États. Bienvenue dans le meilleur des mondes.

(post de Nantes Révoltée)

« Projet Pegasus » : révélations sur un système mondial d'espionnage de téléphones

- « Projet Pegasus » : révélations sur un système mondial d'espionnage de téléphones - « Le Monde » et seize autres rédactions ont eu accès à plus de 50 000 numéros de téléphone potentiellement ciblés par Pegasus, un puissant logiciel espion israélien, pour le compte d'une dizaine d'Etats. Une arme numérique utilisée contre des journalistes, des avocats, des militants et des responsables politiques de nombreux pays, dont la France. (...) La législation internationale n'encadre qu'à la marge les ventes de ces armes informatiques, que leurs acheteurs utilisent quotidiennement contre des civils, et même contre des populations protégées par la convention de Genève, comme les médecins. (...) « Projet Pegasus » n'est pas l'histoire d'un scandale de surveillance de masse, comme l'ont été les révélations d'Edward Snowden sur les opérations menées par la NSA américaine, en 2013. Les victimes de Pegasus ont été ciblées, individuellement, par des gouvernements et des services de renseignement. Mais ces deux scandales ont un point commun : ils montrent à quel point les espions qui utilisent les outils les plus perfectionnés pour surveiller et contrôler les moindres détails de la vie de leurs cibles n'ont jamais de comptes à rendre.
- **Au Maroc comme en France, des journalistes mis sous surveillance avec le logiciel Pegasus** - Les numéros de nombreux journalistes marocains ont été sélectionnés comme cibles potentielles dans le logiciel espion Pegasus. Des journalistes français, dont le fondateur de « Mediapart », Edwy Plenel, et une journaliste du « Monde », ont également été espionnés.
- **Le projet Pegasus : un logiciel espion utilisé par des États pour cibler des politiques, des journalistes, des avocats... y compris des Français** - De nombreux pays utilisent un logiciel espion pour cibler leurs propres concitoyens, ou des représentants d'États censément amis. Plus de 1 000 Français sont concernés. Révélations d'un consortium de journalistes créé par Forbidden Stories, dont fait partie la cellule investigation de Radio France.
- « Projet Pegasus » : quand la dérive devient la norme - Les révélations publiées au long de cette semaine par « Le Monde » et seize rédactions associées au sein du « Projet Pegasus » prouvent, de manière incontestable, qu'en matière de cybersurveillance l'abus est la règle, et non l'exception.
  Editorial. Depuis des années, des réponses invariablement lénifiantes sont opposées aux nombreuses inquiétudes sur les dérives potentiellement liberticides rendues possibles par les outils créés par l'industrie de la surveillance numérique. Les entreprises de ce secteur, comme les Etats qui font appel à leurs services, assurent que les risques sont infimes, les usages encadrés, les engagements respectés. Depuis des années, les doutes sont balayés au nom de l'intérêt supérieur des sécurités nationales, et de la lutte contre le terrorisme ou le crime

organisé.

Cette négation de l'évidence sera désormais beaucoup plus compliquée. Les révélations publiées au long de cette semaine par Le Monde et seize rédactions associées au sein du « Projet Pegasus », coordonnées par l'organisation Forbidden Stories, en partenariat avec Amnesty International, prouvent, de manière incontestable, qu'en matière de cybersurveillance l'abus est la règle, et non l'exception.