

CARNETS DE RECLUSION #2

Dans un premier texte, il était question du parti-état-patron qui est à la pointe de l'innovation scientifique mondiale en matière de contrôle social en Chine. Il est question dans celui-ci de sa déclinaison française.

Le Backtracking pour tous

« La technologie est neutre, c'est l'usage qui en est fait dont il faut surveiller les dérives. » Marc Darmon, directeur général des systèmes d'information et de communication sécurisés chez Thales¹.

Un colonel du Centre de recherche de l'École des officiers de la Gendarmerie a écrit de la reconnaissance faciale qu'elle « ne peut être désinventée » et d'ajouter : « Sous réserve d'algorithmes exempts de biais, elle pourrait mettre fin à des années de polémiques sur le contrôle au faciès puisque le contrôle d'identité serait permanent et général.² »

Nous savons depuis longtemps que sous le couvert idéologique de « modernité », l'innovation est intrinsèquement liée à la survie du capital. Qu'ils en soient conscients ou qu'ils s'ignorent, ses porte-paroles sont nombreux et bien répartis dans l'ensemble de la société. Ainsi, dans *Le Monde* du 14 octobre 2019 et dans *Marianne* quatre jours après, le secrétaire d'État chargé du numérique, Cédric O, faisait valoir le droit d'expérimenter « qui est également nécessaire pour que nos industriels progressent » et pour « ne pas louper le coche technologique ». De ce point de vue, il n'a pas à se faire de souci, un tsunami d'expériences est en cours ici même : reconnaissance faciale dans la rue et détecteurs d'émotions des passagers en scannant leurs visages dans les bus de Nice, capteurs de sons suspects à Saint-Étienne, quantification des déplacements en Ile de France et ailleurs (ce qui a permis de mesurer le récent exode parisien), traçage dans 12 000 pharmacies des achats de médicaments antipyrétiques ou antitussifs comme estimation du nombre de personnes possiblement contaminées. Ne doutons pas un instant que cette industrie plaidera pour un continuum du suivi sécuritaire jusque dans les campagnes, évidemment.

Dans ce domaine, l'innovation est quasi permanente, elle est même déchaînée, étant donné les profits escomptés de par le monde et le peu d'apport en capital fixe nécessaire : il s'agit essentiellement de recherche et développement en intelligence artificielle. Toutes les grandes entreprises – Thales, Cisco, Idemia, issue de la fusion de Morpho et Oberthur, etc. – planchent sur tous les types de tracking possibles, dans tous les domaines. Les entreprises de renseignement Palantir³ et NSO⁴, démarchent les gouvernements en permanence pour traiter leurs données hospitalières ou mesurer la contagiosité de leurs citoyens. La Plateforme intégrée d'opérations conjointes (IJOP en anglais) est une des applications utilisées par la police chinoise pour surveiller les Ouïgours du Xinjiang⁵ : elle les classe par degrés de suspicion pour les envoyer ensuite dans des camps de rééducation. Depuis deux ans et demi, le ministère de l'Intérieur français piaffe d'impatience et se positionne comme futur « maître d'ouvrage et maître d'œuvre de l'élaboration de solutions d'identité numérique⁶ » ; un pas supplémentaire a été franchi dans cette direction le 13 mai 2019 avec la création par décret d'ALICEM (pour Authentification en ligne certifiée sur mobile) qui doit permettre, dans un premier temps, de s'authentifier par le visage pour accéder aux sites comme ceux de la Sécurité sociale et des impôts. N'oublions pas non plus ce que peu ont remarqué : feu la réforme des retraites était « à points ». Pour les *capitaliser* il fallait donc entrer dans le *compte personnel d'activité* (CPA) créé par la loi travail à l'été 2016 et passée inaperçu. De fait, cela constituait une étape importante dans « l'acceptabilité sociale » de la version française du « crédit social à points » établi Chine⁷ ; on pourrait même parler d'une entrée forcée dans ce système de surveillance généralisée auquel un milliard et quatre cents millions de personnes ne peuvent d'ores et déjà plus échapper, où qu'ils habitent dans ce pays. Quant aux gendarmes et policiers français, ils portent depuis quelques temps des caméras piétonnes HIK Vision, une société basée à Hangzhou.

Pour un État qui ne dispose pas d'un puissant parti unique, qu'il soit laïc ou confessionnel, « l'acceptabilité sociale » d'une nouveauté comme disent les sociologues – qu'il s'agisse d'installer une industrie polluante, une surveillance généralisée, une réforme régressive – peut poser problème. Pour y parvenir, il s'agit de mettre en place une stratégie et une tactique accompagnées d'un discours de justification, de le mettre en musique via des communicants et des « éléments de langage » que les médias pourront facilement relayer.

Le schéma est toujours le même : les États justifient les restrictions des libertés et les dispositifs de surveillance par la nécessité de protéger les citoyens d'une menace qu'ils ont eux-mêmes créée ou contribué à créer. Par exemple, cela fait beau temps que l'origine du « sentiment d'insécurité », comme le nomment les médias, n'est plus un mystère. Il ne fait pas doute qu'il est même entretenu : le procès de France-télécom⁸ fut à ce sujet tout à fait éclairant. Et c'est soi-disant pour lutter contre tous les « effets retour » de ces effondrements sociétaux et des destructions délibérées des libertés qui les ont accompagnés, que les états d'exception sont progressivement entrés dans le droit commun.

De manière plus générale, on nous serine depuis des années que la sécurité (que le capital met universellement en cause) est « la première des libertés ». Ainsi, le pyromane se déguise en pompier pour fourguer une marchandise compensatoire destinée à nous rendre toujours un peu plus dépendants, comme le ferait un dealer. Et c'est bien cela qui est projeté, car lorsque tout désir est évacué et que s'établit le règne sans partage des pulsions, alors c'est le signe d'un asservissement accompli.

Dans un premier temps ces « mesures d'urgence » sont toujours déployées à titre dérogatoire ou préventif. Or, dès que resurgit un attentat ou un virus, les préventions sautent, les libertés reculent et les technologies de surveillance gagnent un cran de généralisation. Cela s'appelle la *tactique du cliquet*. À l'origine, il s'agissait d'une innovation d'ordre juridique qui, introduite dans certains textes par les technocrates européens, empêchait toute remise en cause ultérieure, tout retour en arrière, d'où son nom. Après les attentats de 2015, on a prorogé six fois l'état d'urgence, avant de faire basculer un certain nombre de ses mesures dans le droit commun.

Il existe également un *effet cliquet* plus discret : au fil du temps, on mise sur l'accoutumance pour pérenniser des dispositions prises à titre temporaire. Par exemple le plan Vigipirate introduit en 1995 est devenu permanent depuis. Autre exemple, les outils techniques utilisés par les services de sécurité au mépris du droit ont été légalisés par la loi renseignement en 2015.

Le coronavirus peut permettre la mise en place d'un puissant levier d'asservissement

D'autant que cela risque de durer un moment. Dans une interview au Monde du 8 avril 2020, le secrétaire d'Etat au numérique Cédric O et le ministre de la Santé Olivier Véran, ont annoncé qu'ils préparaient une application StopCovid qui permettrait de « retracer l'historique des relations sociales » des personnes infectées et sera présentée à l'Assemblée le 28 avril. « Un outil numérique parmi d'autres dans la lutte contre l'épidémie », a précisé Cédric O, rappelant que l'enrôlement ne se fera que sur la base du volontariat mais qu'au moins 60% de la population devrait la télécharger pour espérer faire baisser le taux de reproduction du virus...

Or, une douzaine de chercheurs de l'Institut national de recherche en sciences et technologies du numérique sont formels : **aucun système, fut-il décentralisé et crypté, n'est en mesure de garantir les droits et libertés de chacun et chacune d'entre nous** au sens du premier alinéa de l'article 1 de la loi de 1978.⁹

Evidemment, le gouvernement Macron joue sur le fait qu'après des semaines de confinement, le backtracking (une expression bien imagée) va faire figure de moindre mal et même de monnaie d'échange contre une libération conditionnelle et sans contact... suspect. Il suffit de voir à quel point certains seraient prêts à accepter l'installation d'une application intrusive pour sortir de ce confinement : *le bracelet électronique plutôt que l'incarcération*¹⁰ et comme ils sont déjà très largement utilisés, on peut avancer que cette pandémie accélérera une dynamique techno-disciplinaire qui la précédait largement. Ainsi, les Etats confieront aux citoyens la responsabilité d'être leurs propres matons et de se surveiller les uns les autres. « Toutes les conditions sont réunies pour transformer les confinés en auxiliaires de police, petits délateurs ou enfermés sacrificiels, garants du respect des règles.¹¹ »

Les lignes bougent jusque chez les plus fervents défenseurs de la privauté sur Internet : le Chaos Computer Club allemand, la plus ancienne organisation de hackers d'Europe, vient ainsi de publier les recommandations qui rendraient *acceptable* le traçage individuel. Il y est écrit :

« L'application et toutes les données recueillies doivent être utilisées *exclusivement* pour lutter contre les chaînes d'infection par le SRAS-CoV-2. Toute autre utilisation doit être techniquement empêchée *dans la mesure du possible et légalement interdite*... Pour une efficacité épidémiologiquement significative, une application de recherche des contacts nécessite un degré élevé de diffusion dans la société. [...] *Les obstacles organisationnels ou juridiques à l'accès aux données ne peuvent pas être considérés comme suffisants dans le climat social actuel de réflexion sur l'état d'urgence et d'éventuelles exceptions de grande portée aux droits constitutionnels par le biais de la loi sur la protection contre les infections.*¹² »

On constate à la lecture de ces passages, l'incroyable naïveté politique des premières lignes mais heureusement cela se termine par un regard plus lucide concernant les éventuels obstacles *organisationnels ou juridiques* qui pourraient être effectivement contournés dans le *climat social actuel... d'urgence et d'éventuelles exceptions de grande portée*. À travers l'usage d'une application numérique, on voudrait aussi nous faire oublier le saccage délibéré du système de santé et nous faire croire que la criminalisation des passants ou la géolocalisation des malades peuvent compenser la pénurie de masques, l'absence de tests, de respirateurs et le manque de personnel. Autrement dit, les états instrumentalisent la question de la santé, (après qu'elle ait été sacrifiée sur l'autel du néolibéralisme) en vue d'anesthésier les désirs de rébellion et l'esprit critique.

Comme il ressort d'un phénomène mondial et incontrôlable en ce moment, les Etats ont compris qu'ils peuvent se servir du SARS-CoV-2 comme d'un puissant pouvoir normalisateur ; ils s'appuient pour ce faire sur une peur légitime (étant donné l'état des systèmes de santé) et sur la mise en place d'une régression sociale couronnée par

un enfermement digne des temps antédiluviens. Ainsi, nous n'avons plus accès à l'espace public que sous des conditions très strictes ; il est comme occupé, « quasi militarisé et devient un laboratoire sécuritaire¹³. » Et nombreux sont ceux qui font à juste titre remarquer que la marchandise, elle, continue de circuler. Par contre, ce qui est moins visible, c'est que notre propre circulation physique pourrait devenir en grande partie accessoire : plus que jamais en ce moment, nos clones se perfectionnent ; car eux ont *l'énorme avantage de pouvoir* circuler à la vitesse de la lumière. *Exit* la fâcheuse et déplorable réalité de nos corps sexués, désirants... et mortels.

Mais le plus puissant ressort sur lequel les pouvoirs peuvent s'appuyer, c'est une figure de la mort que l'on croyait à jamais disparue et que réactualise cette pandémie dont nous ne connaissons la généalogie que dans les grandes lignes, mais dont nous pouvons relater en détail le pourquoi d'une transmission internationale aussi rapide¹⁴. Reste que dans d'autres écrits et à plusieurs reprises nous avons déjà soutenu que la rupture intervenue dans l'histoire de la Terre et du vivant en 1945 fut également le signe d'une inéluctable et radicale évolution du capital, au point qu'il a entraîné depuis lors et sous différentes formes « une guerre généralisée au vivant » que beaucoup refusent encore de voir, pour plusieurs raisons. À leur décharge, il faut dire que tout être humain normalement constitué est amené à refouler le plus loin possible cette question de la mort. Cela pose une difficulté de taille à la critique radicale car dans les années et les décennies qui viennent, la camarade se fera toujours plus présente. Dans ces conditions, comment lever le refoulement de manière à saisir ce qui structure en profondeur la réalité présente ?

Il y a un corollaire à la radicalisation d'un capital qui mène inévitablement le monde vers une issue fatale : il est à craindre qu'au fur et à mesure que cette issue apparaîtra clairement pour ce qu'elle est aux yeux du plus grand nombre, il utilise pour se perpétuer des violences inédites, « coûte que coûte ». Par exemple, et pour paraphraser Sandra Lucbert, *quelle forme pourrait prendre une guerre ?* Eh bien celle-ci, aussi invraisemblable que cela pouvait apparaître il y a encore quelques mois : un bon vieux retour aux guerres inter-impériales façon début du xx^e dont on voit bien quels seraient à présent les deux acteurs principaux. Mais attention, rien à voir avec les armes et les destructions d'il y a un siècle ! Il faut avoir saisi l'incroyable ampleur du projet impérial de Xi Jinping aimablement dénommé « Les nouvelles routes de la soie »¹⁵ pour comprendre que les autres ne se laisseront pas aussi facilement mettre à poil. Le capital a aussi à sa disposition de gigantesques moyens d'asservissements qui lui permettent, comme en Chine, d'envisager un nouveau « design anthropologique des foules », réactualisation d'anciennes convictions eugénistes (dont on voit resurgir les fantômes dans ses lieux d'expérimentation originels, les hôpitaux, lors de l'AktionT4) et totalitaires. Qui aurait dit il y a quelques semaines seulement que, de fait, les états livreraient pieds et poings liés des milliards de « clients captifs » aux GAFAM et à leurs applications ? Sans doute que ce manifestant de Hong-Kong qui se déclarait sous nos yeux ébahis « prêt à mourir pour la démocratie » avait-il confusément saisi cette évolution. Nous n'en sommes pas encore là.

Jean-Marc Royer, le 26 avril 2020

¹ Nathalie Silbert, « Comment la reconnaissance faciale s'installe en France », Les Echos, 15 octobre 2019.

² Olivier Tesquet, Télérama des 8 octobre 2019, 9 et 20 avril 2020.

³ L'entreprise basée à Palo Alto en Californie travaille pour la communauté du renseignement des États-Unis, notamment pour la NSA, la CIA et le FBI, pour différents acteurs du système de défense américain, comme les US Marines, l'US Air force et les Opérations spéciales, ainsi que pour plusieurs services de police comme le NYPD ou le LAPD. En 2016, Palantir obtient en France un contrat avec la Direction générale de la Sécurité intérieure, contrat qui fut renouvelé en novembre 2019. Elle s'est diversifiée dans les secteurs de la finance, de l'assurance, de la santé et des biens de consommation courante. Wikipédia.

⁴ NSO Group Technologies est une entreprise israélienne de sécurité informatique dont les fondateurs sont des anciens membres de l'unité 8200, l'unité de renseignement israélienne responsable du renseignement d'origine électromagnétique. Elle est accusée d'avoir fourni des outils pour espionner des militants des droits de l'homme et des journalistes. Wikipédia.

⁵ Regarder à ce propos le documentaire de Sylvain Louvet, « Tous surveillés. 7 milliards de suspects » sur Arte.

⁶ AFP, « Le ministère va lancer le chantier de l'identité numérique », Le Point du 19 septembre 2017.

⁷ Lire à ce sujet « Coronavirus et dispositifs de contrôle social : l'exemple chinois », Lundimatin n°235 du 23 mars 2020.

⁸ Lire le beau texte de Sandra Lucbert « Procès France-Télécom : Quelle forme peut prendre une guerre » Lundimatin#200, 18 juillet 2019.

⁹ INRIA, « Le traçage anonyme, dangereux oxymore, Analyse de risques à destination des non-spécialistes », 21 avril, télécharger le PDF.

¹⁰ Lire ou relire à ce propos Ira Levin, *Un Bonheur insoutenable*, J'ai lu, 2018.

¹¹ Olivier Tesquet, *articles déjà cités*.

¹² Chaos Computer Club, 10 requirements for the evaluation of "Contact Tracing" apps, 2020-04-06.

¹³ Nicolas Celnik, « Surveillance : l'espace public militarisé devient un laboratoire sécuritaire », Libération du 3 avril 2020.

¹⁴ Nous expliquerons dans un texte ultérieur pourquoi la direction d'ADP a fait de Roissy le Hub du virus en France.

¹⁵ Voir à ce propos le documentaire de Sophie Lepault et Romain Franklin, « Le Monde selon Xi Jinping », Arte, 2018.