La Surveillance des populations – de Scylla en Charybde…

I. Chine – Totalitarisme numérique vertical & Produit d'exportation

Xi Jinping a fixé le cap : la suprématie chinoise en matière d'IA (pour 'Intelligence Artificielle') dès 2030. Mais derrière cette ambition technologique, s'étend un projet politique : celui de mettre sous contrôle, comme nul avant eux, près de 20% des habitants de notre planète. Mao ordonnait qu'on gardât un *œil attentif* sur les contre-révolutionnaires, pour mieux les dénoncer. Xi Jinping a repris l'idée en nommant « Œils attentifs » les centaines de millions de caméras de surveillance dont il couvre son pays. Mais il n'a que faire du vaste réseau de délateurs nécessaire du temps de Mao, il peut compter sur ses meilleures start-ups, sachant que depuis 2015, il a inscrit dans la loi la fusion militaro-civile des Recherches-Développements touchant aux secteurs stratégiques, et à l'IA au premier chef. Le partenariat public-privé est particulièrement proactif dans le domaine de la sécurité, où les entreprises font assaut d'initiatives pour mettre leurs technologies au service du renseignement intérieur.

Pour juguler tout danger politique ou toute déviance économique, il a aussi mis au pas la nouvelle oligarchie du numérique en frappant son représentant le plus 'arrogant' d'une amende colossale et d'une suspension boursière, le tout venant après quelques mois de rééducation forcée. Les 'Quatre Modernisations' lancées en 1978 par Deng Xiaoping n'ont décidément pas vocation à être suivies par la Cinquième tant espérée de la libéralisation politique : le capitalisme chinois croît sous strict dirigisme étatique, les comptes de dépôts seront bientôt gérés par la Banque centrale, les patrons et les ingénieurs sont tenus en laisse, et les données personnelles des milliards de consommateurs d'*Alibaba*, de *Baidu* ou de *WeChat* sont préemptées par la police.

La Chine, dont l'internet est isolé de la toile mondiale sauf à quelques 'portes' aisément contrôlables, est le cadre idéal pour expérimenter une surveillance policière totale. Sa population est ultra-majoritairement connectée avec plus d'un milliard de smartphones. À l'achat, on vous scanne le visage, c'est la loi.

Ainsi de *City Brain*, qui synthétise les flux de données provenant d'une multitude de capteurs répartis dans un environnement urbain. Les progrès en sont un meilleur chronométrage des feux grâce au comptage des voitures, ou de la cadence des métros grâce à celui des voyageurs. De même, les poubelles connectées optimisent la collecte des déchets. *City Brain* peut retrouver les enfants perdus, les bagages des touristes ou les colis de terroristes. Il peut repérer les vagabonds, les sans-abris ou les émeutiers. Toute personne en danger peut se signaler à ses caméras équipant les réverbères, les magasins, les sonnettes de porte, les véhicules automatisés, etc. *City Brain* traite aussi les sons captés par toutes sortes d'objets connectés qui prennent le relais dans les endroits aveugles. Les individus sont reconnus par leur empreinte vocale et leurs paroles sont analysées par des algorithmes policiers.

Il s'en forme un modèle matriciel de la ville mis à jour en temps réel. Quiconque n'y serait pas immédiatement identifié deviendrait suspect. Les autorités disposent à terme d'un profilage sociopolitique universel. À chaque individu peut être associé un crédit politique, variant avec le risque qu'il représente pour le Pouvoir – comparable au 'crédit social' de *Sesame Credit*, une filiale d'*Alibaba*, selon lequel on perd ses droits élémentaires (santé, fiscalité, justice) si l'on a déplu – les erreurs de calcul au détriment du citoyen étant tolérées car, au final, elles poussent à l'autodiscipline.

Un tel système est proposé à l'exportation le long des Nouvelles Routes de la Soie aux autocrates de tous bords. Mais les réalisations d'infrastructure – ports, barrages, liaisons routières et ferroviaires – ne sauraient remodeler l'Histoire autant qu'une telle superstructure numérique, laquelle peut modifier l'équilibre des pouvoirs entre l'individu et l'État sur tous les continents. Il ne s'agit pas là d'un obscur complot mondial mais d'une ambition diplomatique clairement proclamée par la Chine elle-même – quoique ce soit tout récent.

On préférait douter que la Chine puisse intégrer et traiter une telle collecte d'informations. Mais en 2018, un hacker a piraté un programme de reconnaissance faciale qui synthétisait un nombre imprévu de flux. Ce programme, autre production de *City Brain*, profilait les Ouïghours selon leurs 'traits ethniques'. Il identifiait les yeux ou les bouches en toute position ou direction, il faisait abstraction des barbes, des lunettes pare-soleil, enregistrait les numéros de série de tout smartphone passant à portée de chacun, ainsi que la date et l'heure de l'événement. Un tel hacking a apporté une preuve supplémentaire que la Chine utilise directement sa technologie de contrôle dans sa répression des Ouïghours, contre lesquels elle la teste et la renforce.

Si la Chine est déjà couverte de millions de caméras de surveillance, leur densité est la plus forte en pays ouïghour : aucun espace public ne doit leur échapper. Sortir de chez soi, c'est être instantanément identifié, voire être survolé par des drones à forme d'oiseaux. Les images sont associées aux clichés pris par la police lors de 'contrôles sanitaires' durant lesquels sont recueillies d'autres données sur les *corps* ouïghours : identification biométrique, groupe sanguin, empreinte vocale, identification ADN, etc.

Les Ouïghours restent le peuple le plus surveillé de Chine. Ils doivent porter en permanence des mouchards, dans leurs sacs, dans leurs poches ; ils doivent télécharger des applications-espion qui chassent nuit et jour les 'virus idéologiques' ; qui analysent leurs messageries à la recherche d'extraits du Coran et qui signalent les mots en arabe dans leurs fichiers d'images. Nul ne peut s'y soustraire car le cryptage ou les VPN (brouilleurs de navigation) sont interdits.

Le système enregistre toute sortie hors des quartiers de résidence, tout passage dans les banques, les parcs ou les écoles. Dans les rues, les piétons sont identifiés par reconnaissance faciale ; aux stations-essence, ce sont les automobilistes. En sortie de ville, ceux-ci doivent descendre du véhicule afin que leur visage et leur carte d'identité soient une nouvelle fois scannés. La police vérifie les téléphones aux innombrables points de contrôle. Le moindre contact, même indirect, avec quelqu'un qui aurait pénétré dans une mosquée peut coûter la détention. La police consigne tout écart de comportement, et même plus : qu'on ait quitté la maison par l'arrière plutôt que par devant, qu'on passe moins de temps à parler à ses voisins, qu'on consomme davantage d'électricité, possible indice de la présence d'un clandestin. Se passer de technologie ou se tenir à l'écart des réseaux sociaux n'est même pas une solution car l'inactivité numérique elle-même éveille les soupçons.

Au début de l'épidémie de covid-19, tous les Chinois s'étaient vu attribuer une couleur – vert, jaune ou rouge – qui réglait leur liberté de déplacement suivant leur dangerosité sanitaire. De tels codes servent à marquer politiquement les Ouïghours du Xinjiang. Mais contre eux, la sanction est directement politique : c'est la détention et la rééducation.

S'agit-il, à l'échelle du peuple des Ouïghours de Chine, d'un néo-totalitarisme 'exemplaire' – en ce qu'il serait voué à s'étendre à la Chine toute entière, et à s'exporter internationalement ? Hélas, on peut le craindre : la CETC, société d'État qui a fourni le système de surveillance du Xinjiang, se vante d'y avoir établi « les bases solides d'un déploiement national » et elle équipe à présent le Zhejiang et le Guangdong, qui comptent respectivement 57 et 106 millions d'habitants…

II. Démocraties occidentales – Sûreté d'État *vs* Entropie des réseaux

Le contrôle des populations en démocratie est d'une toute autre nature. Mais sous quelles formes s'exerce-t-il, avec un progrès technique s'accélérant à chaque instant ?

Paradoxalement, l'IA fonctionne d'autant mieux qu'on l'alimente massivement en données. Leur concentration par milliards optimise ses capacités de traitement. Fini de crouler sous la quantité, fini les bureaucraties obèses et incapables d'innover. Les régimes policiers, qui structurellement concentrent les données et les décisions, étaient handicapés au 20e siècle. Mais l'IA du 21e leur donne un avantage sélectif, au sens darwinien, sur les sociétés aux pouvoirs séparés, aux acteurs pluriels, aux informations distribuées. Cette prime à la dictature sera-t-elle historiquement décisive ? Poussera-t-elle les démocraties vers toujours plus de centralisation des données et de centralisme tout court, jusqu'à même leur faire prendre l'autoritarisme pour modèle ?

2013, le scandale de la National Security Agency révélé par Edward Snowden. Après le 11 septembre, l'alliance des 'Five Eyes' (Australie, Canada, Royaume-Uni, Nouvelle-Zélande, USA), initialement créée pour espionner le Bloc de l'Est, s'était mise à surveiller ses propres nationaux et ses alliés dans une parfaite illégalité. En France, au cours du seul mois de décembre 2012, 70 millions de communications téléphoniques étaient enregistrées ; en Allemagne, même le portable de la Chancelière Merkel était sur écoute.

Octobre 2001 : le 'Patriot Act' aux États-Unis ; 2015… 2017 : état d'urgence en France et lois antiterroristes à peu près similaires. Avril 2021 : projet de loi prévoyant de « *pérenniser l'utilisation des algorithmes* » (autorisés en 2017) afin d'identifier toute navigation vers des contenus en rapport avec le terrorisme.

L'Histoire aura donc voulu que nos 'sociétés informationnelles' naquissent dans un contexte de lois d'exception. Car c'est au même moment que nous sommes massivement entrés dans l'ère numérique. Un chiffre : *Facebook* (fondé en 2004) : 3,45 milliards d'utilisateurs – 45% de la population mondiale, tous âges confondus. Un autre : *Google* (fondé en 1998) : 2,3 milliards d'usagers mensuels. Il a suffi de 20 ans pour nous retrouver presque tous connectés, entre nous et par nos interactions avec les objets dits « intelligents » c'est-à-dire captant nos faits et gestes. D'ici encore 20 ans, il faudra compter avec les constellations satellitaires et peut-être surtout avec l'ordinateur quantique.

Nos technologies occidentales de surveillance (caméras, drones, biométrie, algorithmes tournant sur super-ordinateurs) valent celles de la Chine. Mais chez nous, c'est démocratiquement que se règle le conflit dialectique entre ces deux besoins naturels, inscrits comme deux Droits humains fondamentaux : la liberté et la sécurité. Or, depuis 2001, nous avons préféré moins de liberté pour plus de sécurité contre le terrorisme.

L'exceptionnalité juridique s'est insinuée dans nos systèmes de lois en même temps que ceux-ci se faisaient déborder par la 'révolution numérique'. Oui, il s'agit bien d'une révolution. Technologique certes, mais économique en ce qu'elle a révélé une nouvelle source de Valeur, qu'elle a fait émerger une classe nouvelle d'oligarques et une inégalité sociale nouvelle ; révolution aussi parce qu'elle a remis en cause tous les droits patiemment élaborés de la personne, de sa vie privée, de la propriété – publique, commune ou privée – de l'information, de la presse, de la souveraineté en matière de communication ou de stockage des données, etc. Ajoutons-y la révolution de la communication politique sur les réseaux et la pression exercée vers toujours plus de dérégulation.

Quoiqu'à la traîne, l'Europe œuvre sans pareille pour que l'ère numérique mérite le nom de 'Civilisation de l'information', c'est-à-dire que cette nouvelle ère s'établisse dans le respect de l'État de Droit. Elle le fait à sa manière : avec sa mémoire des tragédies totalitaires du 20e siècle qui l'ont ravagée, sa pensée du droit politique – en un mot : avec la Loi.

Contre le danger d'un néo-totalitarisme numérique, une Convention, dite « Traité 108 », a été signée dès 1981, portant sur « la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » ; à savoir, toutes les informations se rapportant à une personne physique identifiable ; les données sensibles touchant, elles, plus spécifiquement aux opinions politiques, croyances religieuses, appartenance ethnique, syndicale, situation médicale, condamnations pénales, etc.

À ce jour, le Traité 108 n'a été signé que par 55 des 197 États membres des Nations Unies (28%). On y retrouve toute l'Union européenne avec le Royaume-Uni ; la Turquie ; le Maroc et la Tunisie mais pas l'Algérie ; le Sénégal, le Burkina et Cap-Vert comme seuls signataires africains ; le Mexique et l'Uruguay, seuls de l'Amérique latine ; la Russie et l'Ukraine ; mais aucun pays du Moyen-Orient ; ni le Canada ni les États-Unis ; pas plus que l'Inde, la Chine ni aucun pays du Sud-Est asiatique.

L'Europe a perdu la bataille de l'équipement et du mode de vie de la 1ère génération numérique. Mais elle entend compter dans les batailles qui viennent, de la connexion et du 'cloud' des objets industriels, et du quantique. Son 'Règlement Général de Protection des Données' (2016), tout récemment renforcé par sa 'Législation sur les services et marchés numériques' (DSA & DMA), confirment qu'elle entend regagner en souveraineté et qu'elle s'efforce, quoiqu'encore difficilement mais avec un succès croissant, d'amener les Américains à mieux respecter les droits de la Personne. Comme ses voisines, la France s'est dotée de diverses Hautes Autorités (CNIL, ARCEP-CSA, ANSSI) qui imposent des bonnes pratiques. Les volets numériques des lois d'urgence font l'objet de scrupuleux débats, et toute surveillance policière se fait sous le contrôle des juges. Qu'il faille soumettre la révolution numérique et ses acteurs aux lois et aux valeurs démocratiques, cela fait à peu près consensus ; reste à s'en faire un objectif politique fondamental.

Hantée par son passé et encore renvoyée à lui par la dictature chinoise qui le prolonge, l'Europe est mobilisée contre le risque d'un nouveau totalitarisme 'vertical'. Mais la révolution numérique comporte un autre danger qu'elle peine à identifier, d'autant qu'il est politiquement l'inverse du premier – s'y ajoutant sans l'équilibrer.

La domination numérique des États-Unis se traduit au niveau de puissantes agences de renseignement – qui obéissent, rappelons-le, aux élus d'une nation libre et respectueuse des traités. Mais elle s'exerce aussi très largement via leurs plateformes et leurs réseaux sociaux.

Dans l'urgence de la lutte antiterroriste, ceux-ci ont aidé les agences gouvernementales à collecter de l'information – on a parlé de 'fraternisation' – en échange de quoi ils ont pu croître sans entraves, c'est-à-dire sans nulle surveillance. Et tel est bien le paradoxe : le contrôle policier et militaire a été armé de moyens inédits au moment où s'épanouissait une société civile libérale, mercantile, donnant naissance à des géants qui allaient prospérer dans le secret de leurs algorithmes et le rejet de tout contrôle. C'était ce que Reagan voulait, lui qui, dans son discours d'investiture de 1981, avait fait 'feu sur le quartier général'. Souvenons-nous : « Government is not the solution to our problem; government *is* the problem! » (l'État *est* le problème).

Doit-on donner raison à Shoshana Zuboff, professeure émérite à la Harvard Business School, d'avoir intitulé son essai (fin 2020) « *l'Âge du capitalisme de surveillance* » ? Chacun de nos messages, chaque clic, chaque usage est enregistré et traité par les réseaux, plateformes et autres moteurs de recherche. Nos données personnelles finissent par composer des profils individuels d'une précision inédite, puis sont revendues au plus offrant, y compris les officines politiques. Mais peut-on assimiler cela à une 'surveillance' des populations ? Au sens policier, non ; mais techniquement, et à des fins mercantiles, oui. Le capitalisme de surveillance consisterait donc en un 'contrôle économique' des populations. Dans un premier temps. Car les psychosociologues comme les politologues constatent que, par leur fonctionnement-même, ces services *conditionnent* jusqu'à nos choix intimes ou électoraux, jusqu'à même notre rapport au pouvoir et à la vérité.

Tout se fait avec notre 'consentement' et tout reste gratuit. Pourtant, Zuboff parle d'un véritable 'coup d'État épistémique', qui aurait joué du vide juridique, de l'effet de surprise technologique et psychologique pour fausser notre consentement. La 1ère étape de ce coup d'État serait économique : l'*appropriation privée* de nos données personnelles. Notons le saut théorique, façon Marx, que cela implique : ces données brutes auraient donc intrinsèquement une 'valeur'.

Une telle conception est à l'opposé de celle des géants de la tech, lesquels considèrent que la seule valeur qui soit provient du traitement des données par les algorithmes qui leur appartiennent. En tous cas, notons qu'avec ce néo-capitalisme triomphant, le 'contrôle économique informationnel' des populations est bien devenu la principale source de Valeur.

Révolution pour révolution, Zuboff veut réserver l'utilisation des données aux seules missions de services publics, et interdire leur *extorsion* comme on a interdit l'esclavage, qui soutenait pourtant des économies entières. Mais, une fois redevenues le bien personnel de chacun, faudra-t-il autoriser la vente de ces données ou aller jusqu'à les déclarer 'incessibles' ? Quant aux services : le téléphone est né payant ; il avait été installé sans que les opérateurs n'écoutent ni ne s'approprient les communications. Faudra-t-il en revenir au bon vieux modèle économique du 'juste prix' et sortir d'une gratuité qui s'avère exorbitante ?

La 2e étape du 'Coup' serait l'instauration d'une 'inégalité' (épistémique) radicale entre ce que l'on sait de nous et ce que nous en savons. C'est contre cette inégalité que l'Europe a instauré l'anonymisation des données (hélas, aisément contournable) ainsi que le droit d'accès aux fichiers et le droit d'effacement – qui restent loin de la ratification universelle. Mais remarquons à quel point nous sommes pointilleux dès qu'il s'agit de confier nos données à l'État, et d'une désinvolture parfaite face à des marchands.

La 3e étape serait celle du ‘chaos’ (épistémique) causé par la diffusion massive d’infox et de théories complotistes. *ConspiracyWatch*, qui combat ces processus, le vérifie chaque jour : ne cherchant qu’à fidéliser leurs utilisateurs pour mieux les exposer à la publicité, les réseaux favorisent structurellement l’émotionnel, le sensationnel, le baratin et le mensonge énorme, la violence, la désinformation orchestrée. Ils amplifient les informations corrompues que leurs algorithmes de micro-ciblage dotent d’une efficacité inégalée. Le chaos ainsi créé ne reste pas virtuel : il cause les bulles cognitives, les maladies de l’attention, les addictions, la perte d’engagement social et d’idéaux communs ; il génère le tribalisme, la xénophobie, la défense de ‘réalités alternatives’ au nom d’une interprétation tordue de la liberté d’expression. Et ainsi prospèrent les populistes, se multiplient les meurtres, les jacqueries sans chef ni programme, les élections coup-de-tête, et un jour les marches bien réelles sur le Bundestag ou le Capitole.

Le contrôle économique exercé par ces géants de la tech engendre une entropie politique croissante, c’est-à-dire des comportements de plus en plus ‘incontrôlables’ d’individus ou de groupes peu structurés, rétifs à toute autorité, instituée, ou des experts, ou des savoirs vérifiés, voire même rétifs à tout leadership. Ces géants, devenus à l’échelle mondiale les principaux vecteurs de l’information, de la communication politique et sociétale, font dysfonctionner la démocratie représentative par leur modèle économique-même.

Pour les militaires, le chaos mental devient un but de guerre ; l’esprit humain est leur 6e terrain de conflit – après la terre, la mer, l’air, le cyberespace, et l’espace : « Les techniques civiles se révèlent tout aussi efficaces pour la Défense. Les réseaux sociaux et sources d’information en continu sont des ‘armes de crétinisation massive’, et leurs utilisateurs des ‘idiots numériques utiles’. Il s’agit de définir des stratégies ‘sur-mesure de masse’, pour toucher au socle des valeurs sacrées (morale, religion, culture), tout en offrant d’irrésistibles raccourcis aux circuits individuels de récompense. » Ces mots pourraient avoir été écrits à Moscou ; ils sont ceux de deux experts du Commandement allié de l’OTAN.

4e et dernière étape : Le ‘Capital privé de surveillance’ se substituerait à la gouvernance démocratique. Mais doit-on suivre Zuboff sur ce point ? D’abord, hormis les complotistes, qui irait prêter un agenda politique caché aux présidents d’*Amazon* ou de *Facebook* ? Et puis, même avec retard, les États de Droit sont en train de réagir. Nous avons évoqué les lois européennes ; aux États-Unis, des actions antitrust fédérales contre *Google* et *Facebook* et cinq projets de lois exhaustifs ont été introduits en deux ans. Mêmes avancées aux niveaux des différents États : la Californie – qui gouverne la Silicon Valley – vient ainsi d’adopter une loi historique sur la protection de la vie privée.

Les géants ont un pouvoir de séduction, et une force de frappe financière et de lobbying considérables, mais ils restent légalistes. La seule menace d’un démantèlement anti-trust – qui résoudrait des problèmes de concurrence et d’innovation, mais aucun problème de fond – les a amenés à tomber le masque de leur neutralité technique et à modérer certains contenus, voire même à se doter de Hautes Autorités – hélas, à ce jour, parodiques.

La démocratie ne doit pas avoir peur de son ombre. L’Europe commence à exiger qu’ils ouvrent ‘le capot’ de leurs algorithmes à de véritables Hautes Autorités, installées par les pouvoirs élus ; à des commissions parlementaires assermentées, afin qu’ils respectent les Droits fondamentaux et les principes bien compris de la concorde civile.

La Chine nous menace aujourd'hui d'un totalitarisme numérique orwellien, vertical – comme la haute roche de Scylla. Nous devons aussi lutter contre l'effondrement dans le libertarisme, le populisme et l'anomie des rhizomes – dans les tourbillons de Charybde.

– FIN –

Docteur en sémiolinguistique ; Analyste à *ConspiracyWatch*.

(Le 26 mai 2021 ; 3 400 mots, 22 600 caractères.)