La surveillance par l'IA, un modèle qui se généralise

"Your recent Amazon purchases, Tweet score and location history makes you 23.5% welcome here."

Quand on s'interroge en 2022 sur l'utilisation des traces numériques que nous semons quotidiennement, la lecture du célèbre roman d'anticipation *1984* de George Orwell peut nous sembler bien fade sur certains aspects. Big Brother est aujourd'hui un marché concurrentiel mondial d'entreprises privées spécialisées dans le recueil de données biographiques et leur traitement par des intelligences artificielles. Deux pôles clairement identifiés s'affrontent dans la course à l'innovation : la Chine et les États-Unis. Dans cet article Hélène Jeannin propose une vue d'ensemble des applications et des implications relatives à la généralisation des technologies de surveillance, que favorisent les dynamiques de concentration urbaine de la population mondiale. Big Brother veille autant qu'il surveille au su et au vu de toutes et tous, au point d'orienter les comportements de manière insidieuse. La gouvernementalité algorithmique au service de la révolution anthropologique du néolibéralisme ?

De nouvelles infrastructures matérielles et logicielles amplifient la capacité des États à surveiller les populations. Au moins soixante-quinze pays sur 176 étudiés utilisent activement les technologies d'IA à des

fins de surveillance[1] : plateformes de villes intelligentes/sûres, systèmes biométriques, services de police prédictifs, drones, applications mobiles, capteurs… En outre, dans l'économie numérique en réseau et interconnectée, les actions des individus sont de plus en plus enregistrées et converties en données (*data*). Des modalités différentes mais complémentaires contribuent de la sorte à la généralisation globale de la surveillance.

Les pourvoyeurs de la surveillance

La Chine

La Chine est l'un des principaux moteurs de la surveillance par l'IA dans le monde via ses fabricants (Huawei, Hikvision, Dahua, ZTE…). La reconnaissance faciale, qui s'appuie sur l'identification et l'authentification des visages, s'est immiscée dans la vie quotidienne des Chinois, allant des lieux publics aux distributeurs de papier toilette, régulant ainsi les usages jusque dans l'intimité[2]. Se constituent d'immenses bases de données, informations disparates rassemblées par des groupes privés ou des organismes publics, qu'il faut centraliser, standardiser et rendre interopérables.

L'Initiative chinoise Ceinture et Route[3] (2017) prône l'expansion rapide des technologies de reconnaissance faciale de masse. Elle est soutenue par une subvention gouvernementale de prêts à taux réduits. Elle est favorisée par l'accroissement de la population urbaine au niveau planétaire[4]. Le concept de « smart city », ou ville intelligente, qui abrite, sous un consensus apparent, des philosophies très diverses, lui est particulièrement favorable.

Le modèle de la smart/safe city

La « smart city » s'assortit de promesses visant à proposer des services adaptés aux habitants et rendre la ville plus compétitive et attractive. Une perspective très techno-centrée la considère comme un ensemble de dispositifs techniques capables de remonter des informations utiles pour une planification urbaine automatisée en temps réel[5]. Le recueil, l'analyse et l'exploitation de données sont au cœur même de son fonctionnement – un rôle devenu de plus en plus prégnant au tournant des années 2010 grâce au progrès des disciplines constitutives de l'IA[6].

Un glissement terminologique s'effectue désormais vers la notion de « safe city », où l'un des champs privilégiés d'investissement est adossé à la sécurité urbaine et repose plus sur l'observation des comportements des citadins et la traque des détails[7].

Les démocraties libérales

D'autres entreprises basées dans des démocraties libérales – États-Unis, France, Allemagne, Israël, Japon - jouent également un rôle important dans la prolifération et l'adoption de ces technologies, en vertu d'une corrélation étroite qu'elles entretiennent avec les dépenses militaires d'un pays. Les démocraties libérales sont les principaux utilisateurs de la surveillance par l'IA. La qualité de leur gouvernance devient alors un facteur clé pour éviter toute forme de dérives ou de violations éventuelles[8]. Avec des industries de l'économie informationnelle fortement impliquées (NEC Corporation, IBM, Palantir, Cisco, pour ne citer qu'elles), la Chine n'est donc pas le seul pays à fournir et exploiter des systèmes de surveillance avancés[9].

La surveillance par l'IA, pour …

… contrôler la population

Le rassemblement dans un même lieu (en l'occurrence, la ville) permet aisément le contrôle et la

manipulation[10], une particularité que les auteurs de fiction ont bien saisie[11]. En 1990, Gilles Deleuze décrivait déjà le passage de la société disciplinaire (Foucault), à la société de contrôle, caractérisée par l'importance de l'automatisation informatique[12].

Évaluer chaque technologie de surveillance séparément n'a pas beaucoup de sens. Il faut élargir le questionnement en pensant non seulement la convergence de ces technologies et ce qu'elles produisent en elles-mêmes, mais la manière dont les pratiques sociales s'en emparent[13]. La surveillance a pour vocation le tri social, en vue d'une segmentation et d'un classement des populations, envisagés comme préludes à un traitement différencié[14].

La Chine montre la voie avec son système de crédit social basé sur des points. L'État chinois détient la capacité technique de contrôler étroitement chaque aspect de la vie de ses citoyens. L'objectif déclaré est d'évaluer la « fiabilité » des individus en tenant compte des données personnelles, financières et comportementales, afin de favoriser le contrôle social et de prévenir les instabilités sociales[15].

Pour être efficace, la surveillance est rendue aussi visible que possible. Des modifications comportementales sont créées, même en l'absence de violence physique, en raison de l'omniprésence de la surveillance, de son intériorisation induisant des auto-ajustements, et ce, afin de se prémunir de possibles sanctions. Les États peuvent déployer l'IA pour récompenser les pratiques sociales qui reflètent des modèles de citoyenneté loyale et de nation, tout en isolant et en immobilisant les réfractaires.

... stimuler l'innovation

Au stade actuel de la recherche sur l'IA, « les algorithmes d'IA réussis ont besoin de trois choses : de grandes masses de données, une puissance de calcul, et le travail d'ingénieurs en algorithmes d'IA de bon niveau - mais pas nécessairement d'élite. Pour appliquer la puissance de l'apprentissage profond à de nouveaux problèmes, il faut les trois, mais à l'ère de la mise en œuvre, les données sont au cœur du problème. C'est parce que, une fois que la puissance de calcul et le talent des ingénieurs atteignent un certain seuil, la quantité de données devient décisive [...] »[16].

Or, le crédit social chinois est sans précédent par son ampleur et sa portée. En combinaison avec le plus grand réseau de vidéosurveillance au monde, la collecte d'informations biométriques (échantillons d'ADN et empreintes digitales), et l'introduction obligatoire d'applications de traçage lors de la pandémie Covid-19 depuis mars 2020, il est en passe de devenir une base de données complète sur des centaines de millions d'individus[17].

Globalement, dans tout nouveau type d'autocratie informationnelle (où figurent des pays aussi divers que la Russie de Vladimir Poutine, la Hongrie de Victor Orban, la Turquie de Recep Tayyip Erdo□an, et la Chine), les technologies de surveillance de plus en plus sophistiquées ne servent pas uniquement à garder la population sous contrôle. Les données gouvernementales recueillies par la surveillance deviennent un outil de politique industrielle et constituent un apport pour la recherche et l'innovation[18].

... garantir la suprématie en IA

Une course sino-américaine au leadership mondial de l'IA est engagée.

L'identité du vainqueur dépendra de ce qui sera le plus important pour les orientations de la recherche en IA. Car si les États-Unis conservent la primauté de la qualité et la créativité de leur recherche, en revanche la Chine possède l'avantage du nombre de chercheurs de niveau moyen et d'entrepreneurs de l'Internet. Les institutions de recherche y ont accès à des ensembles de données beaucoup plus vastes et complets que leurs concurrents des pays démocratiques, ce qui pourra engendrer des effets positifs considérables et déterminants pour l'innovation future[19].

Le partage de grandes quantités de données entre l'État et le secteur privé est rendu possible par des réglementations beaucoup plus faibles qu'en Europe ou aux États-Unis[20]. Le système semble également bénéficier d'un haut niveau d'approbation sociale, avec des citoyens indifférents, voire favorables à ce type de surveillance numérique, et des consommateurs moins préoccupés par la confidentialité des données que dans de nombreux autres pays[21].

Le contrôle de la donnée au cœur des inquiétudes

La souveraineté en question

Car le contrôle de la donnée reste au cœur des inquiétudes des pays occidentaux. La gestion par l'État des données de la population nationale ne peut être considérée comme acquise si la souveraineté est partagée, voire transférée, à des entités qui gèrent les données de sa population en son nom.

Le stockage, le traitement et la manipulation des données d'une population par une entreprise étrangère constituent une préoccupation sécuritaire importante. Ils remettent en cause la définition d'une souveraineté étatique limitée aux seuls contours et institutions du territoire. Ils président à la mise en place d'une concurrence entre États et firmes multinationales. Celle-ci se matérialise par des documents de stratégie d'IA des gouvernements et des prises de position réglementaires afin de limiter les risques de vulnérabilité, d'ingérence, et de garder une forme de contrôle.

Le rôle des acteurs du numériques

Les acteurs du numérique américains, les Big Five ou GAFAM (Google, Apple, Facebook, Amazon et Microsoft) sont beaucoup plus internationalisés que leurs homologues chinois, les BATX (Baidu, Alibaba, Tencent et Xiaomi). La pandémie de Covid-19 a accru leur hégémonie dans l'économie globale comme dans le quotidien de leurs utilisateurs. Du fait de leur position dominante, de services multiples (médias sociaux, recherche web, publicités, offres de jeux et de divertissement…), et de modèles économiques engendrant des synergies, ils captent et revendent à d'autres acteurs des quantités phénoménales de données, à partir de dispositifs d'IA de plus en plus nombreux, variés, et performants (assistants numériques personnels, métavers…), sans que les utilisateurs en aient forcément conscience.

Anticiper les risques

L'apprentissage d'une IA dépend de l'accès à un flux constant de données qui ont été codées. Il est arrivé que l'IA code des identités sociales à partir de données historiques ou linguistiques dissimulant des préjugés raciaux, ethniques ou de genre[22], produisant des résultats erronés ou biaisés, préjudiciables et non souhaitables. Ils résultent des problèmes de qualité de données les plus courants : donnée manquante, fausse, contradictoire, incorrectement datée, mal définie, non représentative, illicite, dupliquée, inutile[23]. Des contestations internes de la part de salariés ont terni la réputation de sociétés tout en alertant le public sur les dangers d'applications non régulées et les mésusages de l'IA[24]. Elles ont contribué à une prise de conscience dépassant le seul milieu des ingénieurs et des informaticiens et à la nécessité d'œuvrer pour une IA Responsable bénéfique à l'humanité[25].

Une réflexion sur la surveillance par l'IA, envisagée dans sa complexité, mérite d'y avoir toute sa place.

Notes de bas de page :

[1] Steve Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, septembre 2019.

[2] Frédéric Schaeffer, « En Chine, 1,4 milliards de suspects sous surveillance », *Les Échos*, 6 juin 2018, p. 12.

[3] En anglais, Belt and Road Initiative ou BRI, venu se substituer à la nouvelle route de la soie (2013) pour montrer la multiplicité des liaisons et des tracés.

[4] Cf. Louise Gaxie, Alain Obadia, « Quelles villes pour demain ? », *Silomag*, n° 7, été 2018.

[5] Nathalie Boulanger, Hélène Jeannin, « Une ville intelligente et humaine », Annales des Mines,

Responsabilité et environnement, 2016, n°84, pp. 22-26.

[6] Serge Soudoplatoff, *L'intelligence artificielle : L'expertise partout accessible à tous*, Fondation Pour L'innovation Politique, Paris, 2018, p. 19.

[7] Languillon Raphaël, *De la smart à la safe city, un basculement de (géo)politique imputable à la COVID-19 ?*, La Fabrique de la Cité, 12 juin 2020.

[8] Sur les questions de gouvernance on se référera utilement au guide pratique d'Impact AI (2020) : « IA digne de confiance. Construire une gouvernance adaptée à chaque entreprise ».

[9] Steve Feldstein, ibid.

[10] Michel Foucault, *Surveiller et punir : naissance de la prison*, Gallimard, Paris, 2005.

[11] Hélène Jeannin, « Les représentations fictionnelles de la surveillance », *Ciném'Action*,2013, n° 47, pp. 42-48.

[12] Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle », *L'Autre Journal*, 1990, n°1.

[13] Hélène Jeannin, « Surveillance totale ou servitude volontaire ? », *Interfaces Numériques*, 2015, vol. 4, n° 3, pp. 491-508.

[14] David Lyon, *Surveillance society: monitoring everyday life*, Open university press, Buckingham, 2001.

[15] Genia Kostka, Lukas Antoine, « Fostering Model Citizenship: Behavioral Responses to China's Emerging Social Credit Systems », *Policy & Internet*, 2020, vol. 12, n°3, pp. 256–289.

[16] Kai-Fu Lee, *AI superpowers: China, Silicon Valley, and the new world order*, Houghton Mifflin Harcourt, Boston, 2018, p. 14.

[17] Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State", *Journal of Democracy*, 2019, vol. 30, n° 1, pp. 53-67. *Project MUSE*, doi:10.1353/jod.2019.0004.

[18] Martin Beraja, David Y. Yang, Noam Yuchtma, « Data-Intensive Innovation and the State: Evidence from AI Firms in China », *NBER Working Paper* No. 27723, octobre 2021/ août 2021.

[19] David Karpa, Torben Klarl, Michael Rochlitz, « Artificial Intelligence, Surveillance, and Big Data », Working paper, novembre 2021, à paraître dans *Diginomics Research Perspectives: The Role of Digitalization in Business and Society* (Springer Nature, editor: Lars Hornuf).

[20] Yongxi Chen, Anne Cheung, « The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System », *The Journal of Comparative Law*, 2018, vol. 12, n° 2, pp. 356–378.

[21] Karpa, Klarl et Rochlitz, *ibid*.

[22] Kate Crawford, « Les biais sont devenus le matériel brut de l'IA », *InternetActu/Le Monde*, 3 octobre 2019.

[23] Business & Decision, *Data éthique, IA éthique, les 2 visages d'un futur responsable*, Business & Decision, Paris La Défense, 2019.

[24] Hélène Jeannin, « Le projet Maven : entre postures éthiques et pressions politiques », *A Contrario*, 2019, vol. 2, n° 29, pp. 141-155.

[25] Hélène Jeannin, « L'émergence du mouvement IA responsable dans les organisations : structuration et enjeux », *Communication & management*, 2020, vol. 17, n°2, pp. 105-120.

Pour citer cet article :

Hélène Jeannin, « La surveillance par l'IA, un modèle qui se généralise », *Silomag 15*, juillet 2022. URL : https://silogora.org/la-surveillance-par-lia-un-modele-qui-se-generalise/