Cybernétique et léninisme consultatif
Les deux piliers du pilotage social par les données en Chine

Jean-Baptiste Monnier



Jean-Baptiste Monnier travaille sur les enjeux géopolitiques du numérique au sein d'Asia Centre, un organisme de recherche indépendant à Paris. Son parcours inclut une expérience internationale dans l'industrie du logiciel, notamment en Chine, aux États-Unis et au Royaume-Uni. Titulaire d'un doctorat en ingénierie aérospatiale de l'IIT Chicago et d'un eMBA d'HEC Paris, il fait partie du réseau d'entrepreneurs sociaux Ashoka.

Deux corpus intellectuels, distants en apparence, éclairent ensemble la nature profonde de la gouvernance chinoise sur les données. D'un côté, la cybernétique appliquée à l'État du pionnier Qian Xuesen, théoricien du *systems engineering*, héros de la patrie et père du programme balistique pour l'arme nucléaire chinoise, qui formula dès 1990 l'idée que la complexité sociale ne pouvait être maîtrisée que par la synthèse de données massives – jetant ainsi les bases intellectuelles du système de surveillance. De l'autre, la thèse du politologue Jean-Pierre Cabestan, directeur de recherche émérite au CNRS, sur le « léninisme consultatif » appliqué à la « démocratie populaire intégrale » promue par Xi Jinping. Entre l'ingénieur et le politologue se dessine un troublant dilemme : cette gouvernance des données servirait-elle à émanciper le citoyen ou bien à perfectionner le contrôle du Parti communiste chinois (PCC) ?

Contrairement aux modèles libéraux où les données alimentent les profits des réseaux sociaux sous le regard de pouvoirs publics hésitants entre les droits constitutionnels et la dépendance vis-à-vis des GAFA, le modèle chinois intègre structurellement ces flux au cœur de l'appareil de sécurité de l'État. Dans ce « léninisme consultatif », chaque interaction numérique (message personnel, acte de consommation…) à l'échelle du milliard devient un signal de conformité ou de déviation politique.

Le substrat technique : Qian Xuesen et la société comme système à réguler

Qian Xuesen, un scientifique formé au MIT et à Caltech où il fut professeur et cofondateur du prestigieux Jet Propulsion Laboratory (JPL), est considéré comme l'inspirateur de la surveillance de masse chinoise pour avoir appliqué les principes du *systems engineering* à la société

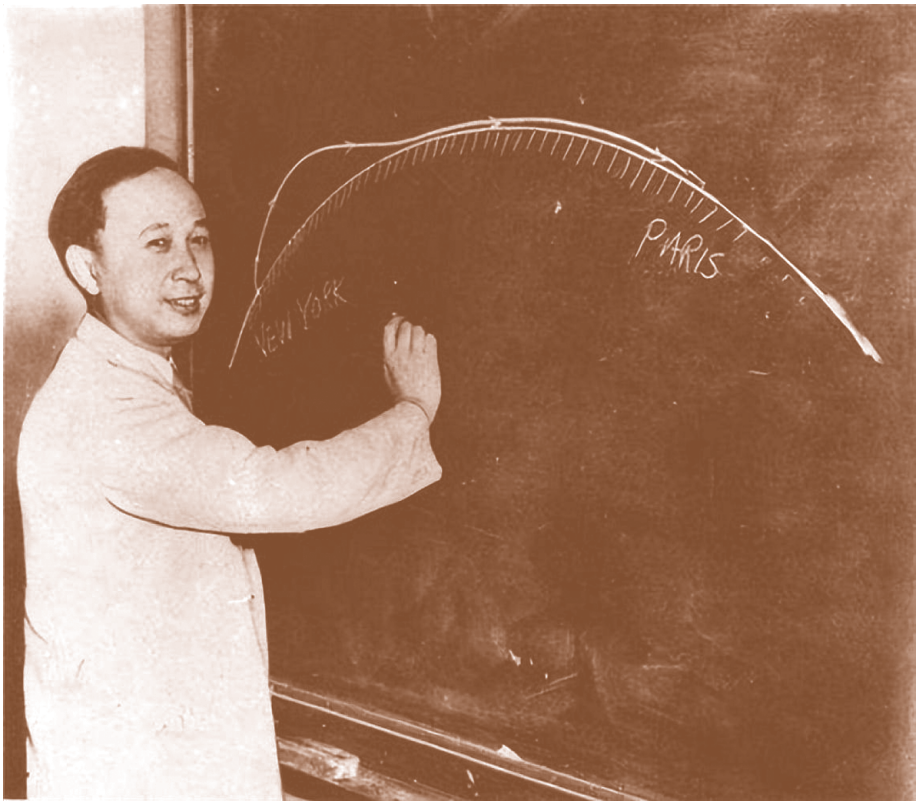


Fig. 1. Qian Xuesen au tableau, Caltech, Pasadena, vers 1944. Domaine public.



Fig. 2. Qian Xuesen reçu par Mao Zedong après son retour en Chine, Pékin, vers 1956-1958. Domaine public.

elle-même, système complexe s'il en est un. Expulsé des États-Unis par le FBI en 1955 après avoir été accusé de sympathies communistes sous le maccarthysme, il a promu sous Deng Xiaoping une approche « métasynthétique » selon laquelle on peut modéliser toute réalité complexe, y compris la société, pour en orienter les comportements. En 1990, Qian soutenait que, pour maintenir le contrôle d'un « système géant

complexe ouvert » comme la société, il était nécessaire de collecter et de synthétiser des quantités massives de données à l'aide d'outils naissants (Qian citait déjà l'intelligence artificielle). Dès lors, la légitimité du gouvernement repose sur l'efficacité scientifique du pilotage plutôt que sur le suffrage universel, un critique chinois notant que ce système a « la jambe scientifique longue et la jambe démocratique courte ». Cette pensée est aujourd'hui intégrée au plus haut niveau de l'État – le président Xi Jinping (ingénieur de formation) ayant déclaré dès 2013 que « l'approfondissement des réformes est un problème d'ingénierie des systèmes complexes » – et l'objectif affiché est de collecter et d'exploiter les données comportementales des citoyens non seulement pour comprendre ou prédire la réalité sociale, mais pour la « guider ».

La construction politique : Jean-Pierre Cabestan et le léninisme consultatif

Selon l'analyse de Jean-Pierre Cabestan sur le « léninisme consultatif », la « démocratie populaire intégrale » de Xi Jinping est avant tout un outil idéologique visant à définir un modèle politique alternatif. Cabestan soutient que cet outil a pour but de « contrer l'hégémonie de la démocratie libérale occidentale » en privilégiant l'efficacité des résultats et le strict contrôle du processus politique. Cependant, Cabestan observe que la consultation citoyenne n'est qu'une façade pour renforcer le contrôle du Parti. Bien que des canaux de participation existent (congrès locaux, enquêtes), ils sont intrinsèquement limités. Le politologue précise que la consultation reste « sélective et exclusivement stimulée par les autorités », sans obligation de résultat ni de responsabilité réelle. Il résume la nature conditionnelle de la participation chinoise par cette autre formule dénuée d'ambigüité : « Si vous êtes obéissant au Parti, vous participez ; sinon, vous êtes exclu. »

Les deux thèses se complètent fonctionnellement. Qian fournit le *mécanisme* – feedback, modélisation, optimisation ; Cabestan décrit le *label* politique qui l'habille et ses limitations.

État des lieux, comment la Chine intervient

L'objectif est affiché : une sécurité intégrée centrée sur le noyau du Parti (le président Xi). Le cadre réglementaire s'appuie sur des outils législatifs – au premier rang desquels la loi sur la Sécurité nationale – qui s'appliquent à tous les acteurs, personnes physiques comme entreprises, mais dont le Parti et la puissance publique sont structurellement exemptés, faute de tout mécanisme de contrôle ou de sanction à leur égard.

Quant à la mise en œuvre aujourd'hui, la machine est lancée avec de nombreux systèmes de contrôle automatique déjà opérationnels : une veille civile détecte les menaces narratives sur les réseaux sociaux, tandis que le réseau Skynet de 800 millions de caméras assure la surveillance physiologique et biométrique (après les premières expérimentations chez les Ouïghours au XinJiang).

Lancé en 2014 par le Conseil d'État, le système de crédit social chinois est un ensemble de dispositifs encore fragmentés visant à renforcer le respect des obligations légales et contractuelles des citoyens et des entreprises. Il repose notamment sur des listes noires administratives et judiciaires, entraînant des sanctions concrètes telles que des restrictions d'accès au crédit ou aux transports. Par analogie, son fonctionnement peut évoquer un permis à points étendu à la vie économique et sociale : les manquements aux obligations (dettes impayées, décisions de justice non exécutées, infractions réglementaires) entraînent des restrictions graduées, tandis que le respect des règles permet de conserver ou restaurer ses droits.

Dans la sphère privée, chaque utilisateur de WeChat – souvent décrit comme l'équivalent combiné de WhatsApp, Facebook et PayPal, avec plus d'1,3 milliard d'utilisateurs actifs – peut choisir librement son avatar et son pseudonyme. Cependant, le principe d'enregistrement sous identité réelle, imposé par la Cyberspace Administration of China (CAC), réduit fortement l'anonymat vis-à-vis des autorités. Cette identification s'inscrit dans un cadre plus large de « gouvernance numérique » et de « gouvernance sociale », dans lequel les autorités disposent d'une capacité accrue à croiser certaines données administratives, judiciaires et issues des plateformes, sans pour autant constituer un système totalement unifié ou centralisé.

Dans le secteur économique, une illustration sera pertinente car dans ce cas, c'est un fleuron français qui en fut la victime. L'affaire Dior débute en mai 2025 lorsque la filiale de Hong Kong fait l'objet d'une cyberattaque, entraînant le piratage de 950 000 fiches clients (noms, téléphones, montants d'achats, etc.). Bien que Dior ait rapidement notifié ses clients et le régulateur hongkongais, l'affaire s'amplifie lorsque le bureau de la Sécurité publique de Shanghai décide d'enquêter sur la filiale chinoise. En septembre 2025, les autorités analysent les données et les méthodes de Dior et prononcent trois sanctions pour violations de la loi sur la Protection des informations personnelles. Double peine pour Dior, l'attaque cyber et les sanctions, mais y a-t-il collusion entre ces deux étapes, Cartier ayant subi les mêmes attaques au même moment ? Une hypothèse est soulevée, la cyberattaque pourrait bien avoir été mise en place par les autorités pour intimider les entreprises exportant des articles de luxe en Chine, d'une part, mais aussi parce qu'elles ont collecté ces informations personnelles, afin de signifier à ces riches clients chinois qu'ils étaient identifiés.

La route de la soie numérique (et autoritaire)

Le modèle chinois de surveillance se distingue fondamentalement de celui des démocraties occidentales. Aux États-Unis ou en Europe, les forces de l'ordre doivent obtenir une autorisation judiciaire pour accéder aux données personnelles d'un individu – mandat, contrôle d'un juge indépendant, procédure contradictoire. En Chine, ce filtre n'existe pas. Le contrôle s'exerce en amont, directement intégré aux plateformes : l'État dispose d'un accès structurel et continu aux données, sans intermédiaire judiciaire. Dans ce système, les BATX – Baidu, Alibaba, Tencent et Xiaomi, les équivalents chinois des GAFAM – se montrent très accommodants, non par choix, mais parce que la loi les y oblige et que leur survie commerciale en dépend.

Deux illustrations viennent à l'esprit : en 2010, Sergey Brin, cofondateur de Google et natif de l'Union soviétique, choisit le retrait plutôt que la compromission. Après avoir subi les cyberattaques de l'opération Aurora, il préfère quitter le marché chinois – à un coût considérable – plutôt que de coopérer à la censure d'État. Plus tard, Meta (Facebook) emprunte la voie inverse. Dès 2014, l'entreprise engage des négociations directes avec Pékin, allant jusqu'à développer des outils de censure et proposant un superviseur des contenus aux ordres du Parti. Le tournant viendra en 2018 : un jour seulement après avoir obtenu l'autorisation d'ouvrir une filiale en Chine, Meta voit cette permission révoquée par la CAC. Son échec est acté en 2019 –Pékin n'ayant jamais voulu d'un acteur qu'il ne pouvait pas contrôler entièrement.

L'ambition de contrôle du PCC ne se limite pas à ses frontières et TikTok inverse le rapport de force : c'est maintenant un modèle chinois qui s'impose mondialement, exportant une logique de gouvernance algorithmique et d'influences politiques. Le Congrès américain avait voté la fermeture de TikTok aux États-Unis pour des raisons de sécurité nationale, mais Trump a réussi à contourner ce vote en mettant en place une vente de complaisance.

Une autre illustration de l'exportation du modèle a été révélée en septembre 2025 par la mise en ligne du « Geedge Leak », un ensemble de 800 Go de documents émanant de la firme de Fang Binxing, le père du Great Firewall chinois. Ce volume massif – équivalent à quatre fois celui de l'affaire Snowden – a exposé l'ampleur et la stratégie de la « route de la soie numérique autoritaire » chinoise. Pékin fournit ainsi des solutions de surveillance et de souveraineté cyber « clé en main » à des régimes autoritaires comme la Russie, le Myanmar, le Pakistan et l'Éthiopie, renforçant le contrôle des données dans ces régions.

L'IA generative, ultime outil de pilotage social

L'IA fait partie des priorités nationales en matière de technologie, et avec des ressources nombreuses et ingénieuses, la Chine rattrape et parfois dépasse son rival américain. L'avènement de l'IA marque un saut d'échelle décisif dans l'architecture de contrôle, faisant de la Chine un laboratoire unique pour la gouvernance par les données.

Les LLMs (grands modèles de langage) – les IA conversationnelles comme ChatGPT – apprennent en ingérant des quantités astronomiques de textes issus d'Internet : articles, livres, forums, encyclopédies. Or Internet regorge d'informations que Pékin a officiellement effacées de sa propre histoire : le massacre de la place Tiananmen est documenté sur Wikipédia en 83 langues, les témoignages sur le Xinjiang, la Révolution culturelle ou les dissidents emprisonnés se comptent en millions de pages. Les LLMs ont tout lu, ces contenus alimentent mécaniquement les modèles d'IA – y compris chinois. Le problème pour Pékin est donc fondamental : comment s'assurer qu'une IA entraînée sur la mémoire du monde réponde aux utilisateurs en ligne avec la doctrine du Parti ?

La réponse est réglementaire et technique. La CAC impose aux éditeurs d'IA nationaux de soumettre chaque modèle à une vérification de conformité politique avant toute mise sur le marché – un examen fondé sur des milliers de questions idéologiques auxquelles le modèle doit répondre « correctement ». Enfin les éditeurs ont créé des outils de censure intelligente capables de détecter et de bloquer en temps réel toute question suspecte et toute réponse déviante que ferait la machine (avant que l'utilisateur ne puisse lire cette réponse).

« Les LLMs ont tout lu, ces contenus alimentent mécaniquement les modèles d'IA – y compris chinois. Le problème pour Pékin est donc fondamental : comment s'assurer qu'une IA entraînée sur la mémoire du monde réponde aux utilisateurs en ligne avec la doctrine du Parti ? »

L'État ne se contente plus de réguler l'IA : il l'utilise comme instrument actif de contrôle, supervisant chaque maillon de la chaîne – la collecte des données, la conception des modèles et leurs usages. L'illustration la plus frappante en est la disparition de l'armée des « 5-mao ». Ce surnom désignait les milliers d'individus payés par l'État 5 mao – soit quelques centimes d'euro – pour inonder les réseaux sociaux de commentaires favorables au Parti, noyer les discussions critiques et contrôler les internautes. Un travail de fourmi, humain et coûteux. Aujourd'hui, des robots pilotés par l'IA effectuent ce travail à une échelle et une vitesse incomparables, sans salaire, sans fatigue et sans risque de défection. La propagande n'est plus seulement censurée en aval – elle est fabriquée en amont, de manière automatisée et industrielle.

La Chine se projette également hors de ses frontières. Forte d'un vivier de talents considérable – près de 47 % des meilleurs chercheurs mondiaux en IA sont chinois et la Chine y détient plus de 50 % des brevets –, elle mise sur les modèles *open source* pour conquérir un marché mondial : ses technologies sont téléchargées par des millions d'institutions et d'entreprises à travers le monde, sans qu'aucune frontière réglementaire s'y oppose. Mais le risque le plus immédiat ne réside pas dans la dissémination de la doctrine du Parti contenue dans ces modèles. Il vient d'une nouvelle génération d'agents IA autonomes – dont OpenClaw est aujourd'hui l'exemple le plus viral – capables d'agir seuls sur les systèmes de leurs utilisateurs : lire des fichiers, envoyer des mails, exécuter des commandes. Ces outils ouvrent une classe de risques entièrement nouvelle : vol de données personnelles, espionnage industriel, atteinte à la propriété intellectuelle et menaces sur la souveraineté numérique des États.

Perfection opérationnelle : le mandat du Ciel 3.0

L'affaiblissement de la croissance économique comme fondement de sa légitimité historique contraint le PCC à réinventer le « mandat du Ciel », cette fois-ci autour d'une exigence de perfection opérationnelle (ou « développement de haute qualité » dans la terminologie officielle). Pour cela, le Parti a engagé une expérimentation sociale à l'échelle du pays, visant le pilotage algorithmique de sa gouvernance par l'exploitation massive des données.

Qualifiée d'« orwellienne » par Jean-Pierre Cabestan, cette vision repose sur une assimilation accélérée des technologies de pointe. Dans cette dynamique, le maintien par le Parti de la maîtrise technologique est vital, non seulement pour des enjeux de souveraineté, mais aussi pour prévenir tout contournement par les citoyens, comme c'est le cas avec

les VPN. Cette entreprise sera donc rythmée par l'accélération de l'innovation technologique, seule capable de mettre en œuvre des politiques sur une échelle du milliard d'habitants.

Historiquement, le PCC a osé des « expériences » sociales d'une taille continentale, dont certaines ont eu des conséquences tragiques (Grand bond en avant, Révolution culturelle). Par une coincidence de l'histoire (ou pas), juste après le retour de Qian Xuesen en Chine, Mao lançait la campagne des « Cent fleurs » (1956), transformant les écrits des intellectuels en outils de leur propre répression lors du mouvement antidroitiste de 1957. Aujourd'hui, le contrôle d'État sur l'expression des citoyens n'a pas changé de nature : il a simplement changé d'échelle, démultiplié par la puissance technologique chinoise. Certains citoyens chinois, peu nombreux, gardent cet épisode historique des Cent fleurs en mémoire, d'autres sont simplement prudents et se méfient du pouvoir, mais tous s'infligent une autocensure systématique. Est-ce que ce serait là un statu quo acceptable pour le pouvoir et pour la population ?

Bibliographie

→ Jean-Pierre CABESTAN, « Big brother in China's social governance: The legacy of Qian Xuesen and the new totalitarianism », *Journal of Contemporary China*, 2020.

→ —, « Xi Jinping and China's whole-process democracy: A new form of consultative Leninism », *China Information*, 39 (1), 2025.

→ Mara HVISTENDAHL, « A revered rocket scientist set in motion China's mass surveillance of its citizens », *Science*, 359, 6381, 2018.

→ Qian XUESEN, *Engineering Cybernetics*, New York, MIT Press, 1954.

→ —, Yu JINGYUAN & Dai RUWEI, « A new discipline of science: The study of Open Complex Giant System and its methodology », *Chinese Journal of Systems Engineering & Electronics*, 4 (2), 1993.