« Lire la Chine »

Internet des Objets, surveillance et gestion sociale en RPC

PIETER VELGHE

RÉSUMÉ : Le programme d'« informatisation » du PCC fait appel à un large éventail de TIC [Technologies de l'Information et de la Communication] pour tout transformer, de la production industrielle à la gestion sociale. L'éventail de technologie polyvalente que représente l'Internet des Objets est donc un élément clé des efforts déployés par les décideurs politiques pour faire progresser la numérisation. Cet article examine les affirmations selon lesquelles la politique chinoise en matière de TIC s'approprie l'Internet des Objets pour améliorer la surveillance et la gestion sociale afin d'accroître la capacité de gouvernance de l'appareil d'État chinois. Enfin, il examine les systèmes de crédit social émergents face au passage à la numérisation et à l'analyse orientée par les données (*data-driven analysis*), ainsi que l'attention accrue accordée à la cybersécurité qui résulte de la dépendance de l'État chinois vis-à-vis de la technologie.

MOTS-CLÉS : Internet des Objets, TIC, informatisation, gestion sociale, surveillance, Système de Crédit Social, cybersécurité, RPC.

Introduction

Depuis le 18e Congrès du Parti, le gouvernement de la république populaire de Chine (RPC) s'est engagé à faire de la numérisation le principal moteur du renforcement de la nation et de l'économie chinoise. Avec le passage à l'administration Xi, toutes les questions relatives à « l'informatisation » (*xinxihua* 信息化) sont devenues la priorité absolue afin de transformer la RPC en « puissance numérique » (*wangluo qiangguo* 网络强国). Grâce à l'appropriation généralisée d'un grand nombre de technologies avancées de l'information et de la communication (TIC), notamment l'Internet mobile, l'analyse de mégadonnées, l'informatique en nuage (ou nuagique, *cloud computing*) et l'Internet des objets (IdO), l'objectif est de créer une économie axée sur l'innovation et d'améliorer la capacité du gouvernement à gouverner (Arsène 2016).

Depuis que la RPC s'est connectée au World Wide Web, la politique du gouvernement a consisté en un exercice d'équilibrage continu afin de supprimer la dissidence et tout « contenu préjudiciable » (*youhai neirong* 有害内容) en ligne, tout en s'arrangeant pour que la censure et d'autres mesures n'entravent pas le développement de l'économie numérique (Tsui 2003). La Chine compte aujourd'hui le plus grand nombre d'utilisateurs d'Internet au monde (CNNIC 2016) et s'enorgueillit d'une communauté dynamique et prospère d'entreprises spécialisées dans les TIC. Dans un contexte où le président Xi prend personnellement en charge un certain nombre d'organismes de réglementation concernant l'Internet et compte tenu des liens étroits entre le Parti et les entreprises Internet chinoises, les dirigeants chinois sont confiants dans leur capacité à maintenir le contrôle et à stimuler la croissance et l'innovation (Hong 2017).

Un volet particulier de la technologie des TIC, l'IdO, a récemment pris une place plus importante dans les plans d'« informatisation ». Cette technologie, en raison de son potentiel révolutionnaire et de son omniprésence éventuelle dans un monde dit « connecté » ou « intelligent », mérite un examen plus approfondi. Contrairement à d'autres technologies de réseau, la technologie IdO permet de connecter à Internet une foule d'« objets » physiques différents – comme les Smartphones, les bracelets intelligents, les serrures connectées, les drones, les véhicules autonomes, les caméras de surveillance ou tout autre appareil doté d'une puce électronique. Une fois connectés, appareils et serveurs échangent des données, fournissant ainsi des informations en temps réel dans de nouveaux domaines et à une échelle potentiellement énorme (Greengard 2015). L'IdO crée un Internet différent, car contrairement à la plupart des applications Web précédentes, ses dispositifs et services ont un impact direct sur le monde physique.

Avec la multiplication d'appareils connectés à Internet qui enregistrent, stockent et échangent une grande variété de données, un nombre croissant d'activités sont consignées (Greengard 2015). Avec l'Internet tel que nous le connaissons aujourd'hui et les appareils connectés déjà utilisés (y compris les Smartphones et les montres connectées, etc.), nous vivons déjà dans « l'âge d'or de la surveillance », selon un éminent spécialiste de l'Internet (Schneier 2015 : 4). L'IdO ne fera qu'aggraver la situation. À mesure qu'Internet s'empare de chaque aspect de notre existence, il soulève également des inquiètudes grandissantes sur son utilisation en tant qu'outil de surveillance et de gestion sociale, de piratage informatique et d'espionnage, ou encore de sabotage et d'activités de guerre (Howard 2015 ; Schneier 2018).

Compte tenu de l'ambivalence des dirigeants chinois en matière de TIC, cet article étudie comment l'IdO s'inscrit précisément dans un programme plus large d'« informatisation ». L'analyse se concentre en particulier sur la façon dont on dit que l'IdO améliore les capacités de surveillance et de gestion sociale de l'État chinois. En premier lieu, nous examinerons les plans actuels du gouvernement pour le développement de l'IdO afin de déterminer comment ce dernier et la technologie connexe sont liés au programme d'« informatisation » ainsi qu'à la surveillance et à la gestion sociale en particulier.

Développer l'IdO chinois

La politique de l'IdO a été lancée sous l'administration Hu-Wen lorsque le premier ministre de l'époque, Wen Jiabao, visita le 7 août 2009 un centre de recherche sur la technologie d'IdO fondé au mois de novembre précédent à Wuxi, dans la province du Jiangsu. Sur place, Wen avait appelé à la création rapide d'un « Centre de détection de l'information » chinois (*chuangan xinxi*

zhongxin 传感信息中心), également connu sous le nom de « Reading China Centre » (*ganzhi Zhongguo zhongxin* 感知中国中心) [1]. Depuis, le parc industriel Wuxi New Area (*Wuxi xin qu* 无锡新区) a été transformé en une « ville modèle du réseau de détection » (*chuanganwang shifan chengshi* 传感网示范城市) avec l'ambition de devenir le premier centre d'innovation en matière d'IdO en Chine et dans le monde (Mei 2009). Le plan ratifié par le Conseil des affaires de l'État et le Ministère de l'Industrie et des Technologies de l'Information (MIIT) identifia le « réseau de détection » comme une « nouvelle technologie haut de gamme à usage global » et élément fondamental de la nouvelle industrie stratégique (MIIT 2012).

Ce plan fut présenté au moment où, selon Hong (2017 : 1755-6), « les décideurs politiques prirent conscience des pièges de l'ancien modèle de croissance et se lancèrent dans des "mesures transitoires" ». Avant le 18e Congrès du Parti, le Conseil des affaires de l'État avait déclaré que l'IdO et les autres TIC devraient être mises à contribution pour promouvoir le développement économique dans un monde sortant d'une crise financière, tandis que le développement des TIC nationales serait également nécessaire pour réduire la dépendance vis-à-vis de la technologie étrangère (Conseil des affaires de l'Etat 2010). Cette approche a été intégrée dans le 12e plan quinquennal, et la nouvelle administration Xi-Li a résolument mis ces plans en avant comme dans le plan « Internet Plus » (*hulianwang+* 互联网+) de 2015. L'IdO, avec l'Internet mobile, les mégadonnées et l'informatique en nuage, y a été reconnu comme un composant essentiel de l'ambition du pays de faire de la Chine une « grande puissance numérique » (Conseil des affaires de l'État 2015a).

L'objectif fixé, par le Conseil des affaires de l'État au début de 2013 de « créer un lot de technologies essentielles » et de mettre en place un prototype de système industriel d'IdO d'ici 2015 (Conseil des affaires de l'État 2013) a indéniablement été atteint. En 2017, près de 2 000 entreprises d'IdO dont la valeur industrielle estimée dépasse 150 milliards de RMB se sont établies dans la seule région de Wuxi (Wuxi 2017). D'autres grandes entreprises de TIC telles que Huawei, Alibaba, Xiaomi, Baidu, Tencent et ZTE, ainsi que les fournisseurs de télécommunications China Unicom, China Telecom et China Mobile, se livrent également une forte concurrence pour conquérir les marchés nationaux et internationaux avec des objets connectés innovants [2]. Le marché de l'IdO en Chine valait jusqu'à 750 milliards de RMB en 2015 et représentait 31% du marché total mondial [3], les investissements chinois continuant à stimuler le boom mondial de l'IdO [4]. Des entreprises dans des domaines aussi divers que les transports, la médecine, l'agriculture, l'armée, la gestion sociale et la sécurité publique mettent en œuvre cette technologie. Les biens de consommation tels que les objets connectés portables, les appareils électroménagers intelligents et les véhicules connectés sont également de plus en plus en demande (GSMA 2015). Compte tenu de la tendance à considérer la numérisation comme un nouveau « pôle de croissance rentable » dans l'économie actuelle (Schiller 2014 : 146), le succès économique attendu de l'IdO va très probablement pousser le programme « informatisation » vers de nombreuses directions inattendues.

Périmètre d'application

L'éventail dans lequel l'IdO est censé être développé et utilisé dans la politique gouvernementale en matière de technologie est très large, et prolonge les plans généraux de « smartisation, amélioration et internetisation » (*zhinenghua, jingxihua, wangluohua* 智能化, 精细化, 网络化) (Conseil des affaires de l'État 2013). Sous l'égide de l'administration Xi, l'« informatisation » est appelée non seulement à inaugurer de nouveaux modes de production et de fabrication (comme c'était également le cas sous l'administration précédente), mais également à transformer ou « moderniser » de nombreux processus sociaux et politiques au moyen de la technologie. Au fur et à mesure que les dispositifs intelligents commencent à imprégner l'industrie et la société, le potentiel du gouvernement chinois à exploiter toutes les données générées, et donc sa capacité à « décrypter » le pays, a énormément augmenté. Les plans gouvernementaux visant à ce que l'IdO soit « bénéfique pour faire progresser la réorientation des modes de production, de vie et de gestion sociale » (Conseil des affaires de l'État 2013) doivent donc être compris comme faisant partie d'un vaste effort du Parti communiste chinois (PCC) pour s'approprier l'influence des TIC afin de « relever les principaux défis du Parti dans la propagande, l'opinion publique et la gestion sociale [en vue de] maintenir la stabilité, d'assurer sa position dominante, d'empêcher une opposition organisée et de renforcer sa discipline interne [5] » (Creemers 2017 : 4).

Pour atteindre cet objectif, la surveillance est devenue une priorité absolue. Depuis que le processus de « sécurisation » de l'État chinois a été lancé dans les années 1990, une grande partie de la capacité de gouvernance du Parti a été établie pour fonctionner comme un outil de « maintien de la stabilité » (*weiwen* 维稳) (Wang et Minzer 2015). Leurs effets sont davantage visibles dans les régions politiquement sensibles telles que le Tibet et le Xinjiang, où des postes de contrôle et des caméras de surveillance omniprésents, équipés des derniers scanners d'iris et de technologie de reconnaissance faciale, empêchent la population locale de mener à bien ses activités quotidiennes. Les habitants du Xinjiang seraient également tenus d'installer un logiciel espion sur leur téléphone mobile qui permet de suivre leurs activités en ligne, ainsi que de graver un code QR contenant leurs données personnelles sur tout couteau qu'ils achètent [6]. Des systèmes similaires se répandent dans le reste du pays au fur et à mesure que des systèmes de police gouvernementaux et des projets de collecte de renseignements utilisant la « gestion en grillage » (*wanggehua guanli* 网格化管理) sont mis en place pour intégrer les TIC à la police traditionnelle de rue, aux services sociaux et aux formes de gestion à la fois coopératives et coercitives [7].

Les autorités sont en mesure de s'appuyer sur une technologie de plus en plus performante pour analyser des quantités toujours plus grandes de données, ce qui donne la possibilité d'accroître la surveillance et d'améliorer

1. Wen Jiabao, « 尽快建立中国传感信息中心 » (Jinkuai jianli Zhongguo chuangan xinxi zhongxin, Création rapide d'un centre de détection de l'information en Chine), *Xinhua*, 5 août 2010.
2. Récemment cependant, les entreprises chinoises de TIC (et en particulier Huawei) ont été confrontées à de nombreuses réactions négatives concernant leurs opérations à l'étranger en raison de leurs liens supposés avec l'État chinois et des risques qui découleraient du contrôle par les entreprises chinoises de la prochaine génération d'infrastructures de l'Internet, comme les réseaux 5G. On s'attend donc à ce que d'autres aspects des activités des entreprises chinoises de TIC, tels que le développement et la vente d'appareils IdO, fassent également l'objet d'un examen plus attentif, notamment en raison de l'intensification des relations entre la Chine et les États-Unis, les deux pays étant engagés dans une « guerre commerciale » et les États-Unis venant à peine de se pencher sur des questions telles que le vol des DPI [droits de la propriété intellectuelle] par la Chine.
3. « China urges fresh standards for the Internet of Things », *ECNS*, 30 décembre 2016, http://www.ecns.cn/business/2016/12-30/239651.shtml (consulté le 8 décembre 2018).
4. Maxwell Cooter, « Chinese investment drives IoT boom », *Techradar.pro*, 9 janvier 2018, https://www.techradar.com/news/chinese-investment-drives-iot-boom (consulté le 8 décembre 2018).
5. Toutes les citations originales sont ici traduites en français (ndt).
6. « China has turned Xinjiang into a police state as a police state like no other », *The Economist*, 31 mai 2018, https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other (consulté le 8 décembre 2018).
7. Samantha Hoffman, « Managing the State : Social Credit, Surveillance and the CCP's Plan for China », *The Jamestown Foundation*, 17 août 2017, https://jamestown.org/program/managing-the-state-social-credit-surveillance-and-the-ccps-plan-for-china/ (consulté le 8 décembre 2018).

les mécanismes de retour d'informations qui leur permettent au final d'agir de manière préventive en cas d'incidents et de troubles sociaux (Schwarck 2018). Grâce à ces méthodes, qui auraient été utilisées dès 2011, le gouvernement a été en mesure de suivre avec précision les déplacements de 17 millions de personnes à Pékin à l'aide du signal émis par leurs téléphones portables [8]. De plus, des réseaux élaborés de vidéosurveillance (CCTV), composés de millions de caméras panoramiques, couvrent la plupart des espaces publics urbains. Le gouvernement se vante même du fait qu'à Pékin, grâce à quelque 30 millions de caméras et à la participation de 4 000 policiers, il parvient à surveiller 100% des voies publiques [9]. Le récent programme « Sharp Eyes » [10] de 2015 (*Xueliang gongcheng* 雪亮工程) vise à atteindre une couverture de 100 % de tous les espaces publics et industries clés de Chine d'ici 2020, en s'appuyant non seulement sur le système de vidéosurveillance mais aussi sur les caméras installées à l'intérieur des appareils intelligents des foyers, comme les télévisions connectées [11].

Les Smartphones, les caméras de surveillance et autres dispositifs intelligents sont tous constitutifs de l'IdO. Puisque le nombre d'appareils intelligents possédé par chaque individu augmente et que les espaces publics sont transformés en « villes intelligentes », de nombreux autres processus seront enregistrées et les activités des individus seront surveillées d'une manière inédite. Tout cela est détaillé dans les documents relatifs à la politique de l'IdO. Par exemple ces derniers mentionnent l'utilisation du réseau électrique avec compteurs communicants aux points d'entrée pour la surveillance, ou l'utilisation de « hautes tours » pour les secours d'urgence, les mécanismes de surveillance couvrant des zones focales pour prévenir les intrusions et améliorer la gestion publique des villes, et la création d'une plate-forme de sécurité publique pour la surveillance, les alertes précoces et les secours d'urgence (MIIT 2012). D'autres fonctions mentionnées dans ces documents consistent à développer des modèles pour la sécurisation d'événements et de lieux importants, le contrôle de tous les véhicules à moteur et la gestion de la population flottante (NDRC *et al.* 2013). Dans ces exemples, l'IdO offre les infrastructures nécessaires au renforcement de la surveillance visé par le gouvernement chinois. Mais le véritable succès des plans d'« informatisation » et de surveillance de la Chine repose sur un plus grand nombre de TIC dans lesquelles la reconnaissance faciale, l'intelligence artificielle (IA) et l'apprentissage automatique sont cruciaux.

Le Conseil des affaires de l'État, par exemple, prétend « soutenir les entreprises de protection de la sécurité pour lancer une coopération avec les entreprises de l'Internet afin de développer et populariser la reconnaissance d'image précise et d'autres technologies d'analyse de données, ainsi que d'améliorer les niveaux de renseignement et de service des produits relatifs à la protection de la sécurité » (Conseil des affaires de l'État 2015b). Le MIIT affirme également « soutenir fortement la recherche applicable au stockage et au traitement de grands volumes de données générées par l'IdO, ainsi qu'au technologies d'exploration de données, d'imagerie intelligente et d'analyse vidéo » (MIIT 2011). La reconnaissance faciale est déjà à l'essai dans de nombreux lieux en Chine. Certaines gares l'utilisent pour vérifier si un billet de train correspond à son titulaire [12], les personnes qui traversent en dehors des passages piétons sont publiquement montrées du doigt dans certaines villes [13] et il sera bientôt possible de payer en montrant simplement son visage [14]. Des technologies connexes comme la reconnaissance vocale ont déjà été utilisées pour identifier les fraudeurs par téléphone [15]. Les entreprises qui travaillent avec le gouvernement et lui fournissent la technologie la plus récente bénéficient manifestement de l'accès à toutes ces données. Dans le seul domaine de la reconnaissance faciale, trois start-ups chinoises (SenseTime, Megvii ou Face++ et Yitu) sont estimées à plus d'un milliard de dollars [16].

« Automatiser » la gestion sociale

Comme indiqué plus haut, une importante motivation sous-tendant nombre de ces développements est la volonté du PCC d'utiliser les technologies les plus avancées pour améliorer sa capacité de gestion sociale afin de maintenir la stabilité politique. Le terme « gestion sociale » est devenu central dans le discours du Parti depuis son utilisation dans le cadre du 11e Plan quinquennal, lorsqu'il est devenu un « objectif clé » (*zhuyao mubiao* 主要目标) pour la gouvernance (Pieke 2012). L'accent mis sur la « gestion » est utilisé pour s'attaquer aux problèmes nés de la nouvelle mobilité et de la stratification sociales d'après les « réformes économiques » (*gaige kaifang* 改革开放). Cette gestion vise à aider de manière proactive à maintenir l'ordre public par la communication et la consultation, et si nécessaire, par la coercition afin de renforcer le contrôle du Parti sur la société (*ibid.*). Sous l'égide de Zhou Yongkang – l'homme largement responsable de l'expansion de l'appareil de sécurité intérieure de la Chine, mais condamné en 2014 pour corruption puis exclus du PCC – la gestion sociale s'est développée pour devenir « une solution globale à toutes sortes de problèmes liés à la stabilité sociale » (*ibid.* : 16). Dans un article du *People's Daily* de 2006 intitulé « Renforcer et améliorer la gestion sociale – promouvoir la stabilité et l'harmonie sociales », Zhou préconisait la construction d'une plate-forme de sécurité publique pour la surveillance, les alertes précoces et les secours d'urgence [17]. Cinq ans plus tard, dans le 11e plan quinquennal, cette idée était développée comme « l'un des principaux piliers de la gestion sociale et du maintien de la stabilité sociale » (*ibid.* : 18).

Le champ lexical utilisé par Zhou, notamment lorsqu'il préconise l'élaboration d'un système d'intervention d'urgence, est directement repris dans de nombreux documents de politique d'« informatisation », y compris dans

8. Leo Lewis, « China mobile phone tracking system attacked as "big brother" surveillance », *The Times*, 4 mars 2011, http://www.theaustralian.com.au/news/world/china-mobile-phone-tracking-system-attacked-as-bigbrother-surveillance/story-e6frg6so-1226015917086 (consulté le 8 décembre 2018).
9. Zhang Jingya 张静雅, « 本事城区郊区城管探头全覆盖 » (*Benshi chengqu jiaoqu jiaoqu chengguan tantou quan fugai*, Les sondes couvrent entièrement notre ville), *Beijing Chenbao*, 3 octobre 2015.
10. La traduction anglaise est gardée ici pour référence (ndt).
11. Qiao Long, « China Aims For Near-Total Surveillance, Including in People's Homes », *Radio Free Asia*, 30 mars 2018, https://www.rfa.org/english/news/china/surveillance-03302018111415.html (consulté le 8 décembre 2018).
12. « Face recognition ticket checking comes to Beijing West Railway Station », *China Daily*, 30 novembre 2016, http://usa.chinadaily.com.cn/china/2016-11/30/content_27529029.htm (consulté le 8 décembre 2018).
13. Meghan Han, « AI Photographs Chinese Jaywalkers ; Shames Them on Public Screens », *Medium*, 9 avril 2018, https://medium.com/syncedreview/ai-photographs-chinese-jaywalkers-shames-them-on-public-screens-ad0a301a46a6 (consulté le 8 décembre 2018).
14. Will Knight, « Paying with Your Face: Face-detecting systems in China now authorize payments, provide access to facilities, and track down criminals. Will other countries follow ? », *MIT Technology Review*, mars/avril 2017, https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/ (consulté le 8 décembre 2018).
15. Samuel Wade, « Minitrue: "Voiceprint Analysis Can Recognize Swindlers" », *China Digital Times*, 28 février 2017, http://chinadigitaltimes.net/2017/02/minitrue-delete-article-voiceprint-analysis-can-recognize-swindlers/ (consulté le 8 décembre 2018).
16. Josh Horwitz, « A Chinese e-commerce giant is becoming a major investor in facial-recognition technology », *Quartz*, 9 avril 2018, https://qz.com/1247511/alibaba-is-now-a-major-investor-in-facial-recognition-startup-sensetime/ (consulté le 8 décembre 2018).
17. Zhou Yongkang 周永康, « 加强和改进社会管理 - 促进社会稳定和谐 » (*Jiaqiang he gaijin shehui guanli - cujin shehui wending hexie*, Renforcer et améliorer la gestion sociale – promouvoir la stabilité et l'harmonie sociales), *Renmin ribao*, 25 octobre 2006.

celui de l'IdO (MIIT 2012 ; NDRC *et al.* 2013). On voit ici les liens entre le programme de « gestion sociale » et les schémas de surveillance mentionnés plus haut. Zhou lui-même a également souligné que certaines des tâches relatives à la gestion sociale, telles que la médiation des conflits ainsi que l'expression des plaintes et de l'opinion publique, pourraient être améliorées par l'utilisation d'Internet (Pieke 2012). Cependant, la gestion sociale va au-delà de la simple surveillance, car son approche holistique de « gestion » de la société, combinée au techno-optimisme du gouvernement chinois, l'incite à toujours trouver des moyens plus performants et complets pour gérer la stabilité sociale.

C'est là qu'interviennent des projets tels que le Système de Crédit Social (*shehui xinyong tixi* 社会信用体系) (SCS). Le SCS est un amalgame de différents systèmes de crédit ou de notation qui est développé et testé par différents acteurs gouvernementaux et privés dans le but de classer les individus ou les entreprises en fonction de certains (mauvais) comportements économiques, sociaux et politiques. Sur la base de ce score ou de ce classement, les utilisateurs se voient, soit récompensés par des remises ou un accès exclusif, soit mis sur liste noire ou refusés d'accès aux prêts bancaires, à certains logements ou à certains modes de transport, par exemple. Étant donné que ces différents systèmes présentent de grandes différences entre eux (par exemple, entre les systèmes gouvernementaux et les systèmes d'entreprises privées basés sur la loyauté ou l'historique de crédit) et qu'ils ne sont pas encore pleinement opérationnels, ou du moins pas à grande échelle ou à l'échelle nationale (malgré ce que certains médias occidentaux rapportent), il est impossible de commenter les critères utilisés pour évaluer, leurs implications, ou encore leur « succès » tels que perçus par l'État ou la population chinoise.

Cependant, on peut affirmer que la manière dont le SCS s'inscrit à la fois dans le programme holistique de « gestion sociale » du gouvernement, qui est basé « non seulement sur la légalité, mais aussi sur la moralité des actions [et de ses acteurs], couvrant la conduite économique, sociale et politique » (Creemers 2018 : 2) et dans son vaste programme d'« informatisation » puisqu'il repose sur les récents progrès en analyse de mégadonnées et d'IA ainsi que sur les énormes quantités de données disponibles dans une Chine en pleine croissance numérique. En particulier avec un IdO en plein développement, « tous les aspects de notre vie – transactionnels, éducatifs, médicaux, légaux, récréatifs et de consommation – laissent une empreinte numérique » [18] ; et des systèmes tels que le SCS, comme tous les grands algorithmes de données, tentent de donner un sens à ces empreintes selon leurs propres critères et intentions. Un autre avantage crucial de l'IdO est qu'il a le potentiel de relier et d'intégrer à la fois des processus en ligne comme ceux qui étaient auparavant hors ligne, ainsi que les institutions gouvernementales et l'industrie, afin d'« automatiser » la gestion sociale (Hoffman 2017). L'importance du partage de données entre différents ministères, entreprises, localités et même l'armée est explicitée dans de nombreuses politiques concernant l'IdO. Pour y parvenir, il faut également construire des centres de données (*data centre*) dans tout le pays, dans l'optique d'« améliorer l'actualité, l'exhaustivité et l'exactitude de l'information » (Conseil des affaires de l'État 2016). De cette façon, les TIC – qui jouent un rôle important pour l'IdO – peuvent s'assurer que « les traditionnelles barrières spatiales, temporelles et quantitatives à la surveillance et au contrôle du comportement individuel soient progressivement surmontées » (Creemers 2017 : 15).

Aller plus loin

Au-delà des plans chinois actuels relatifs à l'« informatisation » et à la « gestion sociale », deux tendances importantes pour l'IdO auront une incidence sur le développement de programmes et de systèmes tels que le SCS. La première est liée à l'évolution des modèles économiques induite par la disponibilité des données générées par les « appareils connectés » et les progrès de l'analyse orientée par les données. Avec l'IdO, il n'est pas seulement question d'« objets connectés» ou d'« attacher un capteur à n'importe quoi », mais plutôt de générer, d'avoir accès et d'analyser de nouveaux et de toujours plus nombreux flux de données (Zuboff 2019). En échelonnant les analyses de données, les entreprises peuvent offrir une utilisation de plus en plus efficace de l'énergie et des ressources, et faire des prédictions sur les futurs comportements. De cette façon, les entreprises peuvent, par exemple, proposer des rabais en fonction de l'utilisation d'un service particulier, ou même de la condition physique. Récemment, l'un des plus anciens et des plus importants assureurs-vie nord-américains a déclaré qu'il cesserait de vendre des assurances vie classiques et qu'il n'offrirait que des contrats interactifs qui permettent de suivre les données médicales au moyen de la technologie portable (habitronique) et des historiques de smartphone [19].

Cette incitation des citoyens à l'« autogestion » (au lieu de recourir à la coercition ou aux moyens pénaux) semble également s'inscrire dans la logique des systèmes de données comportementales tels que le SCS [20], comme c'est le cas avec le modèle néolibéral de responsabilité individuelle dit de la Silicon Valley (souvent en combinaison avec une politique d'austérité). Aucun des deux modèles ne prétend que les facteurs sociétaux ne sont pas déterminants dans le comportement des individus, mais ils impliquent qu'il est beaucoup plus difficile de changer ces facteurs que de changer le comportement de l'individu [21]. La différence réside dans le fait que si le second, dans sa « tentative de déplacer le politique avec une notion d'ordre économique et naturel – neutraliser le conflit politique autour des visions normatives inconciliables de la famille, de la société et de la nation en privilégiant l'ordre du domaine économique » (Harcourt 2015 : 98) – tente de cacher ou de nier sa nature politique, le premier (le SCS et les autres scores de crédit chinois en développement) embrasse précisément le politique pour atteindre l'ordre dans le domaine économique (et social) qu'il poursuit explicitement.

Les « scores de crédit » ou les « scores de consommation » n'ont rien de nouveau en soi. Ils prolifèrent dans les organismes publics et privés depuis les années 1950 afin de « décrire ou prédire les caractéristiques, les habitudes ou les prédilections [des gens] » [22]. Mais il n'est pas surprenant de constater qu'à mesure que de plus en plus de capteurs recueillent des données sur le comportement des individus, que l'analyse statistique axée sur les données continue de s'améliorer et que la confiance des individus dans l'exactitude, l'efficacité et l'objectivité des données concrètes perdure (Boyd

18. Jeremy Daum, « China through a glass, darkly », *China Law Translate*, 24 décembre 2017, https://www.chinalawtranslate.com/seeing-chinese-social-credit-through-a-glass-darkly/?lang=fr (consulté le 8 décembre 2018).
19. Suzanne Barlyn, « Strap on the Fitbit: John Hancock to sell only interactive life insurance », *Reuters*, 19 septembre 2018, https://www.reuters.com/article/us-manulife-financi-john-hancock-lifeins/strap-on-the-fitbit-john-hancock-to-sell-only-interactive-life-insurance-idUSKCN1LZ1WL (consulté le 8 décembre 2018).
20. Samantha Hoffman, « Grasping Power with Both Hands: Social Credit, The Mass Line, and Party Control », *The Jamestown Foundation*, 10 octobre 2018, https://jamestown.org/program/grasping-power-with-both-hands-social-credit-the-mass-line-and-party-control/ (consulté le 8 décembre 2018).
21. Evgeny Morozov, « The rise of data and the death of politics », *The Guardian*, 20 juillet 2014, https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation (consulté le 8 décembre 2018).
22. Pam Dixon et Robert Gellman, « The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future », *World Privacy Forum*, 2 avril 2014, http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf (consulté le 8 décembre 2018).

et Crawford 2012 ; O'Neil 2016), les scores de crédit s'avèreront bientôt irrésistibles pour bien des entreprises et gouvernements, quelles que soient leurs intentions commerciales et politiques.

Une deuxième tendance est le danger de s'appuyer sur la technologie et les données, comme dans les plans chinois d'« informatisation ». Dernièrement, il y a eu un important renforcement de l'attention portée à la cybersécurité ou à propos de la sécurité de l'information (*wangluo anquan* 网络安全 ou *xinxi anquan* 信息安全) dans la politique chinoise, mais le niveau de sécurité des TIC en Chine demeure faible, car il est notoire que les piratages à grande échelle, les fuites de données et les arnaques en ligne sont monnaie courante (Lindsay 2015). Au fur et à mesure que l'IdO prolifère en Chine, assurer ne serait-ce qu'un niveau de sécurité de base s'avérera également difficile, car les dispositifs d'IdO sont en général mal sécurisés, souvent utilisés pendant de longues périodes et manquent généralement d'un mécanisme (indispensable) pour recevoir les mises à jour de sécurité [23]. Lors de récents piratages, des dispositifs d'IdO du monde entier ont été compromis à grande échelle et ont servi pour certaines cyberattaques parmi les plus grandes que l'Internet ait jamais connues [24]. Si des dispositifs d'IdO sont piratés, l'impact sur le monde physique peut être grave et avoir des conséquences potentiellement fatales (Greengard 2015).

Par conséquent, une condition préalable à l'adoption par le gouvernement chinois de l'IdO et d'autres TIC est qu'ils soient « gérables et contrôlables » (*keguan kekong* 可管可控) ainsi que « sûrs et fiables » (*anquan kekao* 安全可靠) (Conseil des affaires de l'État 2013). La Loi sur la cybersécurité et la stratégie nationale de sécurité du cyberespace de 2016 (Comité permanent 2016 ; CAC 2016) a constitué un jalon dans les efforts déployés par les décideurs chinois pour améliorer la cybersécurité en Chine. Cette étape politique importante fait de la cybersécurité la première priorité des plans chinois d'« informatisation ». La Stratégie indique qu'il existe un risque que les infrastructures critiques du pays soient ciblées parce que « les réseaux et les systèmes d'information sont devenus des infrastructures critiques et même des centres névralgiques pour l'économie et la société dans son ensemble », et que les attaques contre ces dernières pourraient alors entraîner « la paralysie des infrastructures critiques en matière d'énergie, de transport, de télécommunications, de finances et autres » (CAC 2016). Au fur et à mesure que l'IdO devient partie intégrante de ce « centre névralgique », sa sécurité est appelée à devenir un sujet majeur pour les décideurs chinois en matière de technologie. La sécurité devient également importante lorsque les données sont partagées entre plusieurs organismes gouvernementaux et externes. Davantage de personnes ayant accès à différents types de données, les risques de fuites et d'atteintes à la sécurité augmentent. Cette précieuse mine de données personnelles et possiblement sensibles devient également une cible de choix pour les services de renseignements et les pirates informatiques étrangers et pourrait devenir une source importante de pouvoir dans les conflits internes au Parti (Zeng 2016).

En conclusion, il est bon de garder à l'esprit qu'un grand nombre des développements politiques décrits ici ou des motivations qui les sous-tendent ne sont pas propres à la Chine et se généraliseront à mesure que la technologie s'améliorera. Ces technologies peuvent offrir des solutions à des problèmes réels et ne doivent pas nécessairement être les signes avant-coureurs d'une dystopie. Il en va de même pour le SCS en développement : certains maux sociétaux provoqués par la période de réforme et d'ouverture ont suscité des préoccupations légitimes pour plus de contrôle. De même, la politique de l'IdO est mise en place pour aider à s'attaquer à certains problèmes très spécifiques et persistants qui affligent la Chine, tels qu'assurer la sécurité alimentaire et celle des ressources, lutter contre la pollution, résoudre les problèmes de circulation récurrents et proposer des bilans de santé aux personnes âgées et aux habitants des régions éloignées (NDRC *et al.* 2013). Toutefois, dans le cadre du programme d'« informatisation », l'IdO et les TIC en général sont de plus en plus souvent cités comme de commodes « hommes à tout faire » offrant une solution rapide à certains des « problèmes difficiles » de la Chine. Si ce solutionnisme numérique peut offrir des résultats positifs à court terme (même s'il n'est pas sans danger en raison, par exemple, de la faible sécurité de l'Internet), il ne peut, à long terme, que modifier de façon permanente les règles du jeu entre le gouvernement et les entreprises vis-à-vis de la population.

Traduit par Caroline Grillot.

Pieter Velghe est sinologue à l'Ambassade de Belgique à Pékin (pietervelghe@msn.com). Les opinions exprimées dans cet article sont propres à l'auteur et ne sauraient engager l'institution à laquelle il appartient.

23. Bruce Schneier, « Regulation of the Internet of Things », *Schneier on Security*, 10 novembre 2016, https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html (consulté le 8 décembre 2018).

24. Brian Krebs, « Hit With Record DDoS », *KrebsOnSecurity*, 21 septembre 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos (consulté le 14 février 2019) ; « Today the web was broken by countless hacked devices – your 60-second summary », *The Register*, 21 October 2016, http://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained (consulté le 8 décembre 2018).

Références

Sources académiques

ARSÈNE, Séverine. 2016. « Global Internet Governance in Chinese Academic Literature : Rebalancing a Hegemonic World Order ? » *China Perspectives* 2 (106) : 25.

BOYD, Danah, et Kate CRAWFORD. 2012. « Critical Questions for Big Data : Provocations for a cultural, technological, and scholarly phenomenon ». *Information, Communication & Society* 15 (5) : 662-79.

China Internet Network Information Centre. 2016. « 第三十八次中国互联网络发展状况统计报告 » (*Di sanshiba ci Zhongguo hulianwangluo fazhan zhuankuang tongji baogao*, 38ème Rapport de Statistiques sur le Développement d'Internet en Chine), juillet 2016.

CREEMERS, Rogier. 2017. « Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century ». *Journal of Contemporary China* 26 (103) : 85-100.

CREEMERS, Rogier. 2018. « China's Social Credit System: An Evolving Practice of Control ». 9 mai 2018, https://ssrn.com/abstract=3175792 (consulté le 14 février 2019).

GREENGARD, Samuel. 2015. *The Internet of Things*. Cambridge : MIT Press.

GSMA. 2015. *How China is scaling the Internet of Things*. GSMA Connected Living Programme, juillet 2015.

HARCOURT, Bernard E. 2015. *Exposed : Desire and Disobedience in the Digital Age*. Londres : Harvard University Press.

HOFFMAN, Samantha. 2017. *Programming China : The Communist Party's Autonomic Approach to Managing State Security*. Thèse de doctorat (dans le dossier de l'auteur).

HONG, Yu. 2017. « Reading the 13th Five-Year Plan : Reflections on China's ICT Policy ». *International Journal of Communication* 11 : 1755-74.

HOWARD, Philip. 2015. *Pax Technica : How the Internet of Things may set us free or lock us up*. New Haven : Yale University Press.

LINDSAY, Jon R. 2015. « The Impact of China on Cybersecurity : Fiction and Friction ». *International Security* 39 (3) : 7-47.

MEI, Fangquan 梅方权. 2009. « 智慧地球与感知中国 – 无联网的发展分析 » (*Zhihui diqiu yu ganzhi zhongguo – wulianwang de fazhan fenxi*, La Terre connectée et le décryptage de la Chine – Analyse du développement de l'Internet des Objets), *Agricultural Internet Information* 12 : 5-21.

O'NEIL, Caty. 2016. *Weapons of Math Destruction : How Big Data Increases Inequality and Threatens Democracy*. New York : Crown.

PIEKE, Frank. 2012. « The Communist Party and social management in China ». *China Information* 26 (2) : 149-65.

SCHILLER, Dan. 2014. *Digital depression : Information technology and economic crisis*. Urbana : University of Illinois Press.

SCHNEIER, Bruce. 2015. *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World*. New York : Norton & Company.

SCHNEIER, Bruce. 2018. *Click Here to Kill Everybody : Security and Survival in a Hyper-connected World*. New York : Norton & Company.

SCHWARCK, Edward. 2018. « Intelligence and Informatization : The Rise of the Ministry of Public Security in Intelligence Work in China ». *The China Journal* 80 (1) : 1-23.

TSUI, Lokman. 2003. « The Panopticon as the antithesis of a space of freedom : Control and regulation of the Internet in China ». *China Information* 17 (2) : 65-82.

WANG, Yuhua, et Carl MINZER. 2015. « The Rise of the Chinese Security State ». *The China Quarterly* 222 : 339.

Wuxi New Area Investment. « 2017世界无联网博览会已在进入准备 » (2017 *shijie wulianwang bolanhui yi zai jinru zhunbei*, Le Salon mondial de l'IdO 2017 commence déjà ses préparatifs), 7 février 2017.

ZENG, Jinghan. 2016. « China's date with big data : will it strengthen or threaten authoritarian rule ? » *International Affairs* 92 (6) : 1443-62.

ZUBOFF, Shoshana. 2019. *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power*. New York : Public Affair.

Documents politiques

Cyberspace Administration of China. 2016. « 国家网络空间安全战略 » (Guojia wangluo kongjian anquan zhanlüe, Stratégie Nationale de Sécurité du Cyberspace), 27 décembre 2016.

Ministère de l'Industrie et des Technologies de l'Information. 2011. « 关于印发无联网"十二五发展规划"的通知 » (Guanyu yinfa wulianwang "shierwu fazhan guihua" de tongzhi, Avis concernant l'impression et la diffusion du "Douzième Plan de Développement" de l'Internet des Objets), 28 novembre 2011.

Ministère de l'Industrie et des Technologies de l'Information. 2012. « 无锡国家传感网创新示范区发展规划纲要 (2012-2020年) » (Wuxi guojia chuanganwang chuangxin shifanqu fazhan guihua gangyao (2012-2020 nian), Aperçu du plan de développement de la zone d'innovation modèle du réseau de détection national de Wuxi (2012-2020)), 17 août 2012.

Commission nationale du développement et de la réforme *et al.* 2013. « 关于印发10个无联网发展专项行动计划的通知 » (Guanyu yinfa shi ge wulianwang fazhan zhuanxiang xingdong jihua de tongzhi, Avis concernant l'impression et la diffusion de 10 plans d'action spéciaux de développement de l'Internet des Objets), 5 septembre 2013.

Comité Permanent de l'Assemblée nationale populaire. 2016. « 网络安全法 » (Wangluo anquan fa, Loi sur la cybersécurité), 7 novembre 2016.

Conseil des affaires de l'État. 2010. « 关于加快培育和发展战略性新型产业的决定 » (Guanyu jiakuai peiyu he fazhan zhanlüexing xinxing chanye de jueding, Décision du Conseil d'État sur l'accélération de la promotion et du développement des industries stratégiques émergentes), 10 octobre 2010.

Conseil des affaires de l'État. 2013. « 关于推进无联网有序健康发展的指导意见 » (Guanyu tuijin wulianwang youxu jiankang fazhan de zhidao yijian, Avis directeurs concernant la promotion du développement ordonné et sain de l'Internet des objets), 5 février 2013.

Conseil des affaires de l'État. 2015. « 2015年政府工作报告 » (2015 nian zhengfu gongzuo baogao, Rapport de travail du gouvernement 2015), 5 mars 2015.

Conseil des affaires de l'État. 2015. « 关于积极推进"互联网+"行动的指导意见 » (Guanyu jiji tuijin "Hulianwang+" xingdong de zhidao yijian, Avis directeurs concernant la promotion vigoureuse des activités d'"Internet Plus"), 5 juillet 2015.

Conseil des affaires de l'État. 2016. « 关于"十三五"国家信息化规划的通知 » (Guanyu "shisanwu" guojia xinxihua guihua de tongzhi, À propos du "13ème plan quinquennal" pour l'informatisation nationale), 27 décembre 2016.