Les enjeux de souveraineté des objets communicants

Par **Didier DANET**
Maître de conférences en sciences de gestion, détaché de l'Université Rennes 1 auprès de l'Académie militaire de Saint-Cyr
Et **Alix DESFORGES**
Chercheuse en postdoctorat à l'Université Paris 8 au sein du projet GEODE (géopolitique de la datasphère)

Introduction

Depuis une dizaine d'année, les débats sur les enjeux de souveraineté à l'ère numérique prolifèrent autant au sein des milieux politiques, stratégiques et académiques. Historiquement, l'expression « souveraineté numérique » a été largement mobilisée en France principalement pour dénoncer la suprématie des entreprises américaines en matière numérique. Toutefois, cette expression en apparence simple cache un concept aux multiples facettes (Danet et Desforges, 2020). Or les enjeux majeurs soulevés par l'irruption et la généralisation des outils et des données numériques pour l'exercice de la souveraineté des États requièrent clarté et précision pour en comprendre les mécanismes et dynamiques. Les objets communicants visent principalement à simplifier et à faciliter un grand nombre de processus et démarches. En apparence souvent anodins, ils bouleversent davantage qu'il n'y parait la vie quotidienne des citoyens, mais aussi des organisations et des États. Ils posent des questions en termes de sécurité et de confidentialité pour les consommateurs et les usagers, mais au-delà soulèvent des enjeux de souveraineté en raison de leur massification et de leur pénétration dans tous les aspects de la vie quotidienne.

Pour cet article, nous avons choisi de nous interroger sur les enjeux soulevés par les objets communicants dans le cadre de la souveraineté dans son sens le plus strict, c'est-à-dire la défense des intérêts de la nation et l'exercice de compétences de l'État (Norodom, 2020a). En quoi l'irruption des objets communicants va-t-elle véritablement changer la manière dont la question de la souveraineté se pose aujourd'hui ? Le changement quantitatif d'échelle est en soi préoccupant : plusieurs milliards d'objets captant et transmettant des données de toutes sortes ne sont pas sans conséquences sur la capacité de l'État à exercer ses prérogatives régaliennes internes et externes.

L'article présentera dans un premier temps une analyse des principaux enjeux de souveraineté soulevés par les objets communicants. Nous y verrons que, loin de générer de nouvelles problématiques, la prolifération en cours des objets communicants vient en réalité accélérer et consolider des dynamiques déjà à l'œuvre dans le processus de numérisation des sociétés humaines, par exemple dans les rapports entre États et entreprises du numérique. Nous reviendrons dans un second temps sur l'exemple de la sonnette connectée d'Amazon, qui illustre parfaitement ces dynamiques.

Objets communicants : l'accélération et le renforcement de dynamiques existantes

La massification des objets communicants et leur utilisation dans tous les pans de la vie quotidienne soulèvent trois principaux enjeux de souveraineté pour les États : la sécurité, la maîtrise des données

et la place d'acteurs privés, au premier rang desquels les grandes entreprises du numérique pour l'exercice des pouvoirs régaliens.

La sécurité des objets communicants

Le premier enjeu soulevé par les objets communicants et leur prolifération est celui de leur cybersécurité. En effet, ces objets, principalement conçus pour la vie quotidienne, le sont souvent bien loin de toute préoccupation de sécurité. Décrits comme le « maillon faible de la cybersécurité » (Benhamou, 2021), les objets communicants constituent autant de nouveaux vecteurs d'attaques pour des acteurs malveillants. De plus en plus d'attaques informatiques, notamment des attaques par déni de service, exploitent la très faible, voire souvent inexistante sécurité des objets communicants. En 2016, l'attaque contre la société de gestion DNS Dyn a rendu inaccessibles un grand nombre de sites Internet tels que Twitter, eBay, Netflix, GitHub ou PayPal [(1)]. L'attaque a mobilisé le *botnet* Mirai, dont l'une des spécificités est d'utiliser les objets communicants non sécurisés pour procéder à des attaques en déni de service. Mirai a compté jusqu'à 600 000 objets connectés (Antonakakis *et al*., 2017).

Ainsi, de par leur vulnérabilité aux attaques informatiques, les objets communicants sont devenus une véritable menace en termes de cybersécurité. Or la combinaison de ces dispositifs aux techniques d'attaques existantes participe à l'élévation générale du niveau de menace affectant la sécurité et la stabilité de l'espace numérique dans son ensemble, et plus largement la sécurité nationale (Douzet et Géry, 2020).

La maîtrise des données mise au défi de la massification des objets communicants

La prolifération d'objets communicants conduit à la massification de la production de données de tous types. Cette massification soulève des questions de sécurité pour les consommateurs et les usagers, mais interroge surtout la maîtrise de ces données. En effet, si certaines de ces données peuvent ne pas être sensibles en apparence (contenu d'un réfrigérateur, kilométrage et heure d'utilisation d'une trottinette, etc.), d'autres sont à l'évidence beaucoup plus sensibles (données de santé ou liées à la sécurité du domicile par exemple). Ces données, générées sans même que nous en ayons conscience, peuvent révéler pourtant beaucoup d'informations, que ce soit sur un individu en particulier, offrant d'énormes opportunités de ciblage à des fins commerciales ou d'espionnage, que sur le fonctionnement général d'une organisation quelle que soit son envergure. Elles participent ainsi pleinement au processus de « datafication généralisée » (Cattaruzza, 2019).

En effet, les données (générées par les objets communicants ou non) reflètent les modes d'organisation sociaux et bouleversent les modes de gouvernement des sociétés, avec l'émergence de « nouvelles formes d'expression du pouvoir qui se développent par le biais des outils numériques » (Cattaruzza, 2019). Parmi ces outils, les objets communicants prennent une place de plus en plus importante, par exemple en matière de contrôle des frontières.

Des acteurs privés aux pouvoirs inédits

Le point commun des données générées par les objets communicants est qu'elles sont quasi exclusivement détenues par des acteurs privés, générant ainsi une situation de dépendance des États dans l'exercice d'un certain nombre de leurs compétences régaliennes, par exemple dans la mise en œuvre de leur droit dans l'espace numérique. Perçue comme un réel risque géopolitique, notamment, en France (Danet et Desforges, 2020), cette dépendance est d'autant plus problématique qu'elle intervient à la faveur d'entreprises souvent étrangères qui sont déjà

(1) *HackRead* (2016), "DDoS attack on DNS; Major sites including GitHub PSN, Twitter suffering outage", 21 octobre, https://www.hackread.com/ddos-attack-dns-sites-suffer-outage/

en situation de quasi-monopole sur le marché du numérique. Ces entreprises, que l'on présente trop souvent sous le simple acronyme GAFAM (Google, Apple, Facebook, Amazon et Microsoft), sont perçues comme déjà aussi puissantes que les États (Nocetti, 2019). Les objets communicants et leur massification viennent de fait alimenter des problématiques déjà bien connues sur les questions numériques et sur la façon dont les États exercent leur souveraineté dans bien des domaines (levée de l'impôt, création de la monnaie, gestion des populations, sécurité nationale, etc.) (Norodom, 2020b). Les objets communicants peuvent renforcer la position d'acteurs privés déjà puissants ; des acteurs majeurs du numérique ne manqueront pas de mettre au point des stratégies en vue d'occuper une place centrale dans ces différents domaines, traditionnellement de la responsabilité des États. Mais le changement d'échelle généré par le volume croissant des objets communicants ouvrira des perspectives inédites en termes de services et de compétences, comme l'illustre l'exemple de la sonnette connectée d'Amazon.

L'exemple d'Amazon et de sa sonnette connectée Ring

Cette évolution est déjà largement engagée, notamment aux États-Unis, comme le montre l'exemple de la sonnette connectée Ring d'Amazon. En lui-même, l'objet est assez simple : une sonnette vidéo raccordée avec système audio bidirectionnel et détection de mouvements, cette dernière fonctionnant également de nuit. L'occupant de l'habitation est informé de la présence de visiteurs, de livreurs ou d'intrus grâce à une application dédiée qu'il peut consulter en étant présent chez lui ou à distance. Moyennant un abonnement spécifique très peu coûteux, la sonnette peut réaliser un enregistrement vidéo qui peut être partagé avec le voisinage sur un site dédié, intitulé précisément "Neighbors".

À partir de ce capteur finalement assez commun, Amazon a développé une stratégie qui la place aujourd'hui au cœur du système policier chargé d'assurer la sécurité des citoyens.

L'interconnexion automatique des sonnettes et les échanges de données qui en résultent (les vidéos enregistrées notamment) contribuent à cristalliser des communautés de citoyens vigilants, le périmètre couvert devenant une sorte de "*gated community*" virtuelle, dont Amazon est l'initiateur et l'architecte. Les données qui remontent de ces dizaines de milliers de capteurs sont utilisées de multiples manières. Prosaïquement, elles permettent à Amazon de contrôler la qualité de ses opérations de livraison (à quelle heure le paquet a-t-il été livré ? L'employé l'a-t-il jeté ou l'a-t-il déposé avec précaution ?). Elles sont également cédées à des "*data brokers*" ou à des sociétés partenaires (Facebook par exemple). Elles peuvent surtout permettre à Amazon de se placer comme un prestataire obligé des services de police.

Ce dernier point est bien évidemment le plus lourd de conséquences pour la mise en œuvre des politiques publiques en matière policière.

Centralisant les vidéos captées par les sonnettes dès lors qu'elles perçoivent un mouvement, Amazon dispose de données très anodines (le chat du voisin est passé devant la maison), mais aussi de données plus importantes pour la prévention et la résolution des délits et des crimes. Telle personne inconnue est passée à plusieurs reprises devant un groupe de maisons qui ont été cambriolées. Elle a suivi tel itinéraire, était présente à telle heure à tel endroit… Tous ces indices sont évidemment précieux pour la police chargée de retrouver et de confondre les auteurs des délits et crimes. Il n'est donc pas étonnant que les partenariats se soient multipliés très rapidement entre Amazon et des services de police, couvrant l'ensemble du territoire des États-Unis. En 2018, 40 partenariats avaient été mis en place ; il en existait plus de 2 000 au début de l'année 2021, avec un taux de progression de l'ordre du doublement chaque année. Seuls deux États américains, le Wyoming et le Montana, États ruraux s'il en est, n'avaient pas encore de liens avec Amazon.

La nature et les modalités de ces liens montrent la position centrale de l'entreprise par rapport aux autorités policières.

Tout d'abord, l'entreprise qui collecte les données, en particulier les vidéos, exerce un contrôle de l'accès des services de police à la base qui les contient. Ces derniers peuvent demander à les consulter dans un cadre extrajudiciaire et dans des conditions définies par Amazon. Récemment, l'entreprise a décidé d'instituer des règles de « transparence », la police devant solliciter la consultation par une demande écrite motivée qui sera communiquée aux utilisateurs concernés. Les consultations peuvent également intervenir dans un cadre judiciaire, les modalités étant alors définies par les règles de la procédure pénale, les fameux "*subpoenas*" (ordre d'un juge pour la production d'une pièce ou d'un témoignage). Mais, même dans ce cas, Amazon semble se montrer soucieuse du contrôle de ses bases de données puisqu'elle n'aurait satisfait qu'à moins de 60 % des requêtes judiciaires en 2020.

Surtout, cette maîtrise des données s'accompagne du monopole des outils permettant de les exploiter. Amazon a en effet conçu un logiciel de reconnaissance d'images, Rekognition, qui fonctionne comme un service en nuage ("*cloud-based software as a service*"). Ce service propose nombre de fonctions parmi lesquelles la détection et l'analyse de visages (sexe, tranche d'âge, port de lunettes, émotions…), ou la reconnaissance et l'identification de visages sur des photos ou des vidéos. L'utilité de ce type de logiciel couplé avec les bases de données rassemblées grâce aux sonnettes Ring n'est guère difficile à saisir. Elle n'a d'ailleurs pas échappé aux services de police qui ont été jusqu'à 2020 des clients importants d'Amazon. Mais, l'utilisation du service pour identifier des manifestants du mouvement Black Lives Matter enregistrés par des sonnettes connectées associées à des biais manifestes dans le traitement des images des Noirs américains a conduit l'entreprise à un moratoire renouvelé en mai 2021. Ce moratoire a été suivi par les concurrents d'Amazon, en particulier Microsoft.

Cela revient à dire qu'une entreprise privée, Amazon, se trouve en situation de monopoliser des bases de données immenses, alimentées par des dizaines de milliers de caméras installées à la porte des habitations sur tout le territoire des États-Unis, et elle se réserve l'usage exclusif des logiciels de reconnaissance faciale permettant d'identifier et de tracer toute personne « suspectée » d'avoir commis un « délit », pouvant aller de la livraison non conforme d'un colis à la participation à une manifestation non autorisée ou à un cambriolage nocturne avec violence sur personnes. Mieux équipée et mieux informée que les services de police, elle ne peut qu'en devenir le partenaire obligé, et un partenaire en position de force.

On retrouverait des dynamiques comparables dans d'autres fonctions régaliennes où des acteurs privés pourraient, dans les années qui viennent, chercher à asseoir sur leur capacité d'innovation dans les objets communicants des stratégies visant à occuper une position centrale par rapport aux acteurs publics, qui avaient traditionnellement la maîtrise de la conception et de la mise en œuvre des politiques de l'État. Que l'on songe par exemple à Apple et aux données transmises par les 100 millions de porteurs d'iWatch sur leur activité physique, leur rythme cardiaque ou leur taux d'oxygène dans le sang. Compte tenu du rythme de progression des ventes et de la part d'Apple sur le marché (plus de 50 %, soit cinq fois plus que le deuxième), on peut prédire sans grande difficulté que l'entreprise disposera très rapidement d'un volume de données de santé sans équivalent, et de la capacité à les analyser pour concevoir des services de santé publique.

Conclusion

Au-delà de son aspect quantitatif, l'augmentation brutale du volume des données captées et transmises, la massification à venir des objets communicants devrait s'accompagner de stratégies d'acteurs privés, les entreprises géantes du numérique, pour intervenir dans la conception et

la conduite des politiques publiques, notamment des politiques régaliennes comme la défense et la sécurité, la monnaie ou la santé. On peut penser que ces entreprises chercheront moins à s'approprier la souveraineté des États qu'à se poser en partenaires incontournables des évolutions possibles de ces politiques. Les situations conflictuelles ne sont pas à exclure, comme l'a montré le cas de l'application TousAntiCovid, mais les relations entre acteurs publics et privés seront probablement plutôt de nature partenariale, les États ayant besoin des bases de données et des compétences analytiques des entreprises pour définir les politiques adaptées.

Bibliographie

ANTONAKAKIS M. *et al.* (2017), "Understanding the Mirai Botnet", *Proceedings of the 26th USENIX Security Symposium*, pp. 1093-1110.

BENHAMOU B. (dir.) (2021), *Internet des objets & souveraineté numérique*, Paris, Institut de la souveraineté numérique et AFNIC.

CATTRUZZA A. (2019), *Géopolitique des données numériques,* Paris, Le Cavalier Bleu.

DANET D. & DESFORGES A. (2020), « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », *Hérodote*, n°177-178, pp. 179-195.

DOUZET F. & GERY A. (2020), « Le cyberespace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace », *Hérodote*, n°177-178, pp. 329-349.

NOCETTI J. (2020), « Les Gafam sont-ils trop puissants ? », *Les Grands dossiers de diplomatie*, n°50, pp. 88-89.

NORODOM A-T. (2020a), « Être ou ne pas être souverain, en droit, à l'ère numérique », *in* CASTET-RENARD *et al.* (éd.), *Enjeux internationaux des activités numériques,* Larcier, pp. 21-41.

NORODOM A-T. (2020b), « La souveraineté au défi des plateformes numériques », *in* RAPP L. (éd.), *Le droit international : entre espaces et territoires*, Institut francophone pour la justice et la démocratie, pp. 181-198.