

Les enjeux de souveraineté des objets communicants

Didier DANET Alix DESFORGES
Enjeux numériques – N°16 – décembre 2021
(extraits)

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 coeur 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 oeuvre 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 oeuvre 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.