L'INTERNET DES OBJETS ET LA DATA

STRATÉGIE D'ENTREPRISE

FRÉDÉRIC SCIBETTA
YVON MOYSAN
ÉRIC DOSQUET
FRÉDÉRIC DOSQUET

L'INTERNET DES OBJETS ET LA DATA

L'intelligence artificielle comme rupture stratégique

Préface d'Antoine Denoix

DUNOD

Graphisme de couverture : Hokus Pokus
Illustration de couverture : © Elenabsl/Shutterstock

11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-077237-7

Sommaire

Préface

Un même ouvrage sur l'IoT (Internet of Things) et l'IA (Intelligence Artificielle) ? À première vue, l'exercice relève de la gageure, tant ces deux acronymes semblent, depuis plusieurs années, suivre des destins croisés, voire opposés.

Lorsque j'ai rejoint AXA début 2014, il n'était question, sur le marché, que d'objets connectés. Dans les voitures, à la maison, autour du poignet… et dans un jour pas si lointain (qui sait ?) sous la peau ! Pas un acteur du monde industriel, comme celui du service, ne pouvait rester immobile sur le sujet. Les consultants, moult slides sous le bras, proposaient et vendaient des POC (*Proof of Concept*) en pagaille. Quelques années après, que reste-t-il de cette grande frénésie collective ? D'un point de vue business, pas grand-chose, rien de très impactant. Notre paysage économique ne s'est pas trouvé brusquement transformé, comme il l'avait été par Internet et l'écran connecté, il y a quelques années. La bulle s'est brusquement dégonflée, jusqu'à faire croire à certains que les objets connectés avaient aussi disparu. Excès inverse. Car ils n'ont pas disparu, au contraire. À l'évidence, la connexion va quitter l'écran pour migrer vers les objets, de façon massive. La grande erreur des premières années, commise par le marché, c'est d'avoir poussé l'outil avant de penser l'usage. Ce n'est pas parce qu'on « peut » connecter une brosse à dents qu'il « faut » la connecter et la vendre. Nous avons collectivement perdu de vue l'essentiel, à savoir la question « à quoi ça sert ? ». Et les Français ne s'y sont pas trompés. À quelques exceptions

près, les taux d'équipement des objets connectés sont restés bas. Pour l'IoT, l'essentiel commence : d'abord détecter l'irritant client, puis penser une solution… et avoir recours, de fait, aux objets connectés. Le fait de viser dès le départ la « juste » proposition de valeur fera la différence entre les acteurs économiques qui se gargarisent de concepts, et ceux qui créent les véritables opportunités business.

En 2018, le phénomène IA connaît la même embellie que l'IoT en 2014. Méfiance ! D'autant que la société française, dans son ensemble, s'est emparée du sujet. Chaque semaine, pas une couverture de nos grands magazines qui ne surfe sur le phénomène, en évoquant « robots », « fin du travail », « algorithmes tueurs » et autres joyeusetés ! L'intelligence artificielle se prête aux fantasmes, et elle rencontre toute une littérature de science-fiction, dont nous sommes familiers : Blade Runner, le retour ! Là encore, ne nous trompons pas : l'IA va bien changer nos vies quotidiennes, nos métiers comme nos entreprises. Mais nous n'en sommes encore qu'aux prémices, et il faut se méfier des prophéties auto-réalisatrices des GAFA et autres BAT chinois. Ne perdons pas notre esprit critique. Et retenons l'enseignement de l'IoT : quelle valeur d'usage ?

Le point commun entre l'IoT et l'IA, c'est bien la data. Et l'impérieuse nécessité, pour les marketeurs, les DSI et les dirigeants dans leur ensemble, de la collecter et la comprendre certes, mais surtout de lui donner son sens, son utilité, pour le client final. Ce challenge, il ne fallait pas moins que quatre passionnants auteurs pour le relever et le réussir. Bonne lecture !

Antoine Denoix
Directeur Marketing, Digital et Service Client, AXA France

Introduction

Le monde change vite. Très vite. La génération qui a vécu les premiers pas de l'homme sur la Lune sur les écrans noirs et blancs d'un tube cathodique explore aujourd'hui en temps réel d'autres territoires tout autant challengeant mais beaucoup plus proches – nos champs, nos villes, nos voitures, nos habitats, nos corps, nos cerveaux et bientôt nos pensées.

Nous expérimentons une des plus formidables accélérations que notre humanité n'ait jamais connues. Déjà, nous n'imaginons plus une vie sans Internet, sans mobile. Nous sommes devenus impatients et avides de connaissances, souvent futiles, cordon ombilical qui nous relie à une matrice informationnelle globale, qui sait tout de nous, peut-être plus que nous sur nous-même.

L'Internet des objets est partout ! Évolution naturelle de la très longue chaîne d'innovation des télécommunications, il offre à nos contemporains, en temps réel, une connexion et une interaction entre la mécanique et le biologique. Il est également le collecteur des « Big Data », nouveau pétrole de l'ère numérique, matière brute raffinée par les Data scientists.

Après plusieurs années d'existence, soutenues par un marketing astucieux, l'Internet des objets est maintenant rentré dans son deuxième âge, celui de la raison. Le marché s'organise ainsi autour de plusieurs acteurs de la chaîne de valeur aujourd'hui matures.

Les réseaux offrent une couverture suffisante pour les premiers cas d'usages à grande échelle. Les capteurs de moins en moins coûteux collectent des données en direction de plateformes de plus en plus matures. Les marques, enfin, construisent un panel d'offres de plus en plus larges, de plus en plus hardies en direction de clients finaux de plus en plus éduqués à un bénéfice concret.

C'est ainsi un autre monde qui s'ouvre à notre humanité. Les objets initialement construits pour une action mécanique à finalité limitée se voient investis d'une utilité complémentaire, celle de reporter leur activité et, *in fine,* d'en produire une valeur, notamment en agissant, parfois même préventivement.

Se réalisent ainsi les croyances ancestrales, celles des animistes et des poètes. À cette question de Lamartine « Objets inanimés, avez-vous donc une âme », le XXI^e^ siècle offre une réponse multiple.

Ce sont d'abord nos ouvrages de génie civil, nos routes, nos ponts ou nos canalisations qui se connectent aux grandes plateformes IoT gérées par les grands silos manufacturiers – Microsoft, Google ou Amazon, pour n'en citer qu'une poignée. Les bénéfices en sont immédiats. C'est une maintenance ajustée aux seuls points à traiter qui s'organise ainsi, parfois même de façon prédictive, comme optimisation de l'outil de production et vecteur de croissance économique.

C'est également notre rapport au biologique, à nos corps qui est en train d'évoluer. Nous devenons des « hommes augmentés », entités biologiques mesurées et quantifiées dans chacune de nos actions – notre sommeil, notre activité physique, nos consommations alimentaires – et facilitées dans nos interactions avec les machines – dans l'authentification notamment. Toutes ces données signeront un nouveau profil numérique et finalement une identité et un ADN. Elles constitueront également une nouvelle manière de nous objectiver et de nous comprendre pour mieux interagir avec un environnement toujours plus digitalisé. L'homme augmenté sera plus en phase avec ses outils de production

professionnelle, sa mobilité urbaine et son capital santé. La valeur produite par les données, et affichée sur les nouvelles interfaces mixtes ou augmentées, permettra des gains de productivité ainsi qu'une pénibilité moindre au travail.

Derrière ces évolutions se dessine une nouvelle entité avec laquelle les hommes et les machines interagiront. L'intelligence artificielle, entité auto-apprenante, instruite par nos données et interagissant par de nouvelles interfaces naturelles comme la voix, permettra à tout à chacun de rentrer dans cette nouvelle révolution.

Les nouveaux paradigmes posés par la révolution de l'Internet des objets constituent à la fois une menace fondamentale et de formidables opportunités.

La menace est simple : rester une marque du XX^{e} siècle qui n'aura pas su prendre le virage des nouvelles opportunités du numérique. La sanction en est tout aussi simple : disparaître au profit d'acteurs plus véloces, parfois beaucoup plus récents, et plus proches du centre de gravité de la valeur.

Les opportunités sont multiples. C'est d'abord l'occasion de se repenser dans la chaîne de valeur, c'est-à-dire de se réinventer au regard des nouvelles attentes du marché et des nouvelles opportunités de croissances. La maxime de Henry Ford (1863-1947), industriel et fondateur de la marque automobile éponyme, illustre le challenge : « Si je n'avais écouté que mes clients, j'aurais inventé un cheval plus rapide ».

La deuxième opportunité est de repenser les nouveaux paradigmes et de se mettre en capacité de s'y adapter. L'instantanéité proposée par l'Internet des objets, parfois dans une grande brutalité, oblige à de nouvelles organisations du travail, plus agiles, plus réactives et construites autour du client. Cette mutation s'impose aujourd'hui à un spectre très large d'acteurs, y compris les entités publiques et parapubliques. S'opère ici une mutation Schumpétérienne de renouvellement des organisations par la création, puis la destruction, de nouveaux emplois.

Enfin, l'émergence des outils de captation et de valorisation de la donnée oblige à refondre le marketing et les systèmes d'informations

à l'aune d'un « legacy », un héritage parfois lourd dans un contexte technologique en mutation rapide. Penser à dix ans avec des marques technologiques dont la pérennité et la pertinence ne sont pas assurées à l'horizon d'une poignée d'années est la quadrature du cercle que doivent résoudre les DSI sous l'amicale pression des CMO et CDO voire des CEO.

Les auteurs de cet ouvrage ont voulu mettre en avant les nouveaux paradigmes de ce que le consensus appelle « révolution ». Ils s'appuient sur une vision théorique et pratique proposée par des universitaires et des opérationnels au centre de la transition numérique. De nombreux avis d'experts seront également proposés. Des entrepreneurs, des chercheurs, des juristes et des opérationnels apporteront un témoignage *in vivo* de la réalité, des contraintes et des opportunités soulevées par l'Internet des objets au cœur des entreprises.

Chapitre 1

Une perception holistique de l'Internet des objets

Executive Summary

- **L'Internet des objets** est un concept fourre-tout qui appelle une clarification.
- **La chaîne de valeur comprend le capteur**, le réseau, la plateforme de stockage et de valorisation des données, les outils clients interfaçant avec une machine ou un humain.
- **L'ensemble s'applique des champs à la ville**, du domicile au travail, de son corps à ses véhicules.

Le grand angle : Urbi et Orbi

Les objets connectés sont partout… ou presque. Dans la recherche académique, on admet, les concernant, la définition de Porter et Heppelmann, qui date de 2014. La date même de cette définition montre à quel point, ces objets sont contemporains et ouvrent le champ des possibles d'un point de vue tant scientifique que managérial. Trois éléments ont été retenus pour les qualifier : des composants physiques, des composants intelligents (exemple : capteur) et des composants de connectivité.

Leur existence accentue la fracture numérique à l'échelle planétaire. On considère que 67 % des objets connectés dans le monde seront consommés dans trois pôles : Chine, Amérique du Nord et Europe de l'Ouest. D'un côté, il y aura donc les utilisateurs, et de l'autre, ceux qui n'ont pas imaginé à quel point ces objets représentaient « une nouvelle révolution numérique »[1], voire encore celles et ceux qui opposent une résistance absolue à l'intrusion de la technologie[2].

Mais au-delà de cette segmentation et d'un point de vue citoyen, la dichotomie la plus importante opposera d'un côté ceux qui pilotent les objets et les plateformes pour en tirer toute la valeur ajoutée, et de l'autre, ceux qui n'en seront que de simples utilisateurs.

En effet, dans un monde connecté, le vrai pouvoir appartient à ceux qui stockent et comprennent l'information récoltée. *Data is the new oil* et ce, d'autant plus que les sources de données délivrent gratuitement ces informations. Lancelot-Miltgen et Gauzente (2006) voyaient déjà dans la collecte et la gestion de données une source de gains très appréciable pour les entreprises : « l'exploitation de l'information consommateur est désormais devenue la première source de valeur ».

---

1 Acas R., Barquissau E., Boulvert Y-M., Dosquet E., Dosquet F., Pirotte J., *Objets connectés, la nouvelle révolution numérique*, ENI, 2016.

2 Bagozzi, R P., Lee, K.H., « Consumer Resistance To, and Acceptance Of, Innovations », *Advances in Consumer Research*, Volume 26, p. 218-225, 1999.

Chalomon I., Chouk I., Guiot D., « La cyber-résistance du consommateur : quels enjeux pour l'entreprise ? » *Décisions Marketing*, 68, p. 83-88, 2012.

Roux D., « La résistance du consommateur : proposition d'un cadre d'analyse », *Recherche et applications en Marketing*, 22, 4, p. 59-80, 2007.

L'émergence des objets connectés dans nos sociétés pose aussi des questions juridiques fondamentales quant à la liberté des individus. Les principaux risques recensés dans la littérature varient de trois (Eilstein, Pozuelos, 2016) à six (Chouk, I., Mani, Z., 2016).

En premier lieu, celui de la sécurité notamment liée au piratage des données récoltées par un tiers non autorisé.

Deuxièmement, l'atteinte et la violation de la vie privée, en cas d'utilisation non-autorisée de données personnelles à de multiples fins, commerciales et autres.

En troisième lieu, le risque d'une défaillance technique due par exemple à un bug informatique, qui entraînerait des conséquences négatives dues à des informations erronées.

Ensuite, le risque psychologique. L'intrusion dans sa vie privée est dommageable et peut dans certains cas nuire gravement à l'individu. Afin d'atténuer ce risque, des organismes de régulation comme la Cnil en France opère une surveillance des réseaux.

Cinquième risque, celui lié aux ondes nécessaires à la transmission des informations. Certaines études scientifiques (Anses, 2016) ont montré la nocivité de ce type d'objets, surtout pour ceux en contact direct avec le corps comme les bracelets.

Enfin, le risque financier n'est pas à négliger. Ces objets sont onéreux et entraînent des surconsommations de forfait de transmission, voire électrique, qui peuvent se révéler dommageables pour le consommateur.

Les dispositifs juridiques dans les différents pays industrialisés étaient jusqu'à présent relativement faibles et donnaient surtout l'impression d'être non pas dans l'anticipation, mais en retard par rapport aux avancées technologiques et commerciales. Cette situation était vraie jusqu'à ce que le Parlement européen ne vote le Règlement Général de la Protection des Données (RGPD) en mai 2016 avec une application dès mai 2018. Ce texte permet de combler un vide juridique et de mettre un terme aux problématiques d'exploitation sans contrôle des données personnelles. Ce texte apparaît comme une révolution légale, décidée par le législateur et l'exécutif européens désireux de protéger le

citoyen européen devant la menace d'une exploitation sans précédent des données personnelles à des fins commerciales. Ce texte accorde à toute personne la capacité d'agir vis-à-vis de tout responsable ou sous-traitant d'un système de traitement automatisé de données (STAD).

La base de ce règlement est le consentement éclairé et univoque de l'individu à bien vouloir que les données collectées sur sa personne puissent être traitées avec son plein accord. Selon le baromètre Opinion Way (2017), les consommateurs français sont pleinement conscients de ce risque d'intrusion. Pour 42 % d'entre eux, ils sont méfiants quant à la confidentialité des données collectées, ce qui les freine dans leurs achats d'objets connectés.

Le risque de l'intrusion dans la vie privée n'est d'ailleurs pas l'unique problématique d'une généralisation des objets connectés dans la vie quotidienne. Il existe également le risque lié à l'insécurité. Prenons l'exemple des montres connectées. En Allemagne, l'Autorité fédérale d'encadrement du Web les a interdites à l'école en novembre 2017, et ce n'est qu'un début ; d'autres pays comme la France pourraient lui emboîter le pas. Déjà en 2015, le rapport de HP avançait que les montres connectées auditées dans son étude présentaient cinq types de manquements à la sécurité :

– Identification utilisateur insuffisante. Les dix montres évaluées étaient toutes connectées à une interface mobile qui ne requiert pas d'authentification forte à deux facteurs et ne prévoit pas de blocage du compte après 3 à 5 saisies de mot de passe erroné. Par ailleurs, trois de ces montres n'exigeaient pas de mots de passe suffisamment longs et complexes. HP pointe également le manque de sécurité des procédures de récupération d'un mot de passe oublié. Tout ceci combiné pourrait faciliter le travail d'un cyberpirate.
– Faiblesse du chiffrement dans le transport des données. Ces montres transmettent beaucoup d'informations vers le smartphone auquel elles sont associées, ainsi qu'à des applications mobiles qui les relaient à des services en ligne. Si toutes les montres testées ont bien recours à un chiffrement type SSL/TLS, 40 % des connexions