

Le conflit des souverainetés : Apple et le FBI

Description

[Baisse des prix et importance nouvelle de la data dans la stratégie d'Apple](#) [Apple ne partage pas ses données avec le FBI afin de conserver ses clients](#)

Apple doit trouver les moyens de diversifier son chiffre d'affaires, trop dépendant des seules ventes d'iPhone, ce qui se traduit par l'importance nouvelle accordée aux services et aux données personnelles des utilisateurs d'iPhone.

Dans ce contexte, Apple s'efforce en gardien du respect de la vie privée, ce qui l'a conduit à s'opposer aux demandes d'un juge américain concernant le déverrouillage de l'iPhone de l'un des terroristes de la fusillade de San Bernardino. Régulé par un tiers qui a permis de hacker l'iPhone concerné, cette affaire aurait pu être l'occasion d'établir une doctrine claire afin d'articuler le droit à la vie privée et l'exigence de sécurité.

A l'occasion de la publication de ses résultats pour le dernier trimestre 2015, Apple a franchi un nouveau record : l'entreprise a réalisé un profit net de 18,4 milliards de dollars, un chiffre jamais atteint par aucune entreprise jusqu'alors. Et, pourtant, les ventes d'iPad et celles de Mac sont en baisse, les ventes d'iPhone restent, avec une croissance toutefois limitée à 1 %. C'est le paradoxe d'Apple : la puissance de l'entreprise est liée aux ventes d'iPhone, qui la menacent en la rendant dépendante d'un unique produit.

En 2014, les ventes d'iPhone représentaient quelque 50 % du chiffre d'affaires d'Apple, et 66 % en 2015, pour plus de 70 % des bénéfices de l'entreprise. Certes, l'entreprise, positionnée sur le haut de gamme, a absorbé, en 2015, 92 % des bénéfices du marché mondial des smartphones, mais cette performance exceptionnelle ne suffit pas à rassurer les investisseurs. Ce qui a conduit Apple à être détrôné en Bourse par Google en février 2016, l'entreprise à l'origine du moteur de recherche étant devenue la première capitalisation boursière au monde depuis qu'elle a précisé la répartition de ses activités avec la création de la holding Alphabet ([voir La rem n°36, p.58](#)).

[Baisse des prix et importance nouvelle de la data dans la stratégie d'Apple](#)

Cette fragilité d'Apple est manifeste depuis 2012, l'année où l'entreprise est devenue la première capitalisation boursière au monde, date à laquelle son cours a pourtant commencé à évoluer en dents de scie ([voir La rem n°25, p.62](#)). Les investisseurs reprochent au groupe californien de

ne pas parvenir à créer de nouveaux marchés, comme il l'eût fait avec l'iPod et iTunes en 2001-2003, ou encore avec l'iPhone et l'AppStore en 2007-2008.

C'est donc la première fois qu'Apple propose un nouvel iPhone moins cher que les précédents

Aussi faut-il lire dans les récentes annonces d'Apple une réponse aux difficultés stratégiques de la firme liée à sa dépendance à un mono-produit. En effet, Apple a semble-t-il brisé un tabou, le 21 mars 2016, en présentant un nouvel iPhone baptisé SE. Il s'agit d'une version de l'iPhone 5S, améliorée par l'apport des processeurs conçus pour l'iPhone 6S Plus, lancé en septembre 2015.

Cette nouvelle version a la particularité de proposer un écran de 4 pouces, contre 5,5 pouces pour l'iPhone 6S Plus, qui se rapproche d'une phablette. Mais surtout, l'iPhone SE est commercialisé à 489 euros, quand l'iPhone 6 est commercialisé à partir de 639 euros et l'iPhone 6 Plus à partir de 749 euros. C'est donc la première fois qu'Apple propose un nouvel iPhone moins cher que les précédents et accepte le principe d'une descente en gamme, même si le prix de l'iPhone SE le positionne encore dans le haut de gamme.

Cet iPhone meilleur marché doit aider Apple à relancer ses ventes, alors que le marché mondial des smartphones voit sa croissance fortement ralentir, celle-ci n'étant que de 0,2 % au premier trimestre 2016. D'ailleurs, sur le premier trimestre 2016, les ventes d'iPhone ont reculé de 16,3 % selon IDC, indiquant la nécessité pour Apple d'une réaction d'ampleur. L'iPhone SE doit inverser cette tendance en élargissant sa base de clients, notamment en Chine et en Inde, des pays où se retrouvent de nombreux primo-acheteurs de smartphones qui n'optent pas forcément pour les modèles les plus chers. Sur les marchés matures, l'iPhone SE doit aussi fidéliser ceux qui pourraient être tentés par la concurrence, des smartphones de qualité existant d'ordinaire à 200 euros.

En effet, la durée de renouvellement des smartphones augmente dans les pays développés, signe de l'attentisme de la clientèle, qui revoit progressivement ses priorités et reporte la décision d'achat. Ainsi, aux Etats-Unis, le cycle de renouvellement des smartphones est-il passé de 23 à 27 mois en deux ans selon RBC Capital Markets. Et c'est peut-être là l'enjeu principal de l'iPhone SE, à savoir fidéliser la clientèle existante en lui permettant de renouveler ses équipements Apple sans devoir augmenter la mise à chaque nouveau modèle d'iPhone. L'iPhone SE viendrait en fait remplacer des iPhone de plus de deux ans, à savoir les modèles de type iPhone 5C et 5S.

Il s'agit ici d'un aspect important de la stratégie d'Apple. En effet, l'une des solutions d'Apple pour limiter sa dépendance aux ventes d'iPhone passe par le développement de

nouveaux revenus, qui supposent toutefois l'existence d'une communauté fidèle. Ainsi Apple communique-t-il de plus en plus sur ses revenus dans les services, l'AppStore, iCloud ou encore Apple Music ayant généré 20 milliards de dollars de chiffre d'affaires en 2015.

Il s'agirait encore d'un repositionnement stratégique majeur, les services (iTunes, AppStore) ayant historiquement eu pour principale fonction de valoriser les terminaux de la firme, ce à quoi correspond d'ailleurs Apple Music qui prend le relais d'iTunes dans le domaine de la musique (voir [La rem, n°37, p.60](#)). Or ces nouveaux revenus commencent à compter significativement dans le chiffre d'affaires d'Apple, pouvant conduire la firme à se positionner, comme Google, Facebook ou Amazon, parmi les entreprises disposant d'une connaissance fine de leurs clients, grâce à la maîtrise des données personnelles.

Apple est même originaire en gardien des données personnelles grâce à son dispositif technique

Or cette connaissance fine des utilisateurs Apple, grâce aux services qu'ils consomment, pourrait demain compter plus que la puissance de la marque Apple, incarnée dans le design de ses terminaux et dans la communication qui accompagne chaque lancement de produit.

Cet enjeu stratégique nouveau pour Apple explique en grande partie la résistance ouverte et médiatisée aux demandes du FBI quand ce dernier a souhaité accéder aux données contenues sur l'iPhone de Syed Rizwan Farook, l'un des terroristes impliqués dans la fusillade de San Bernardino en Californie, le 2 décembre 2015.

Apple ne partage pas ses données avec le FBI afin de conserver ses clients

L'élimination du terroriste lors de l'intervention des forces de police a confronté le FBI à un problème, celui de l'accès à son iPhone protégé par un mot de passe, associé à un identifiant unique logé au sein du téléphone, seul moyen de lire les contenus du téléphone autrement cryptés.

A cela s'ajoute la possibilité pour les utilisateurs d'iPhone d'activer une option qui conduit à supprimer l'ensemble des contenus du téléphone après dix mots de passe incorrects. Sans le mot de passe, le FBI ne peut donc opter pour un déverrouillage du téléphone par la force brute, à savoir le test de toutes les combinaisons possibles de lettres et chiffres. Par ailleurs, Apple ne stocke pas sur un serveur les mots de passe des possesseurs d'iPhone afin d'éviter tout risque de piratage de leurs données, autant de mesures prises à la suite des révélations d'Edward Snowden en 2013, qui ont mis en lumière l'étendue des pratiques par la NSA (Agence américaine de sécurité nationale). Ainsi, depuis la version du système d'exploitation pour iPhone iOS8, toutes les données sont chiffrées par défaut et le code secret de déchiffrement connu de chaque utilisateur uniquement, ce qui garantit à Apple de ne pas avoir à communiquer ces informations aux services de renseignement, à défaut d'en disposer.

Ce type de stratégie, alliant chiffrement et reconnaissance de l'utilisateur depuis le téléphone (par un mot de passe ou une empreinte digitale) a été l'une des principales réponses des géants de l'électronique et de l'internet aux inquiétudes de leurs consommateurs, qui ont découvert pouvoir être espionnés sans trop de difficultés. Apple s'est même originaire en gardien des données personnelles grâce à son dispositif technique, donc aussi en gardien des libertés individuelles, au moins de l'une d'entre elles, le droit de tout individu au respect de sa vie privée. Sauf que l'efficacité du dispositif vaut aussi pour tous ceux qui s'en emparent afin d'échanger des informations en lien avec des entreprises criminelles et qui échappent ainsi aux services d'écoute des agences nationales de renseignement.

C'est dans ce contexte que la juge californienne Sheri Pym a, le 16 février 2016, mis en demeure Apple, lui demandant d'apporter « une assistance technique raisonnable » au FBI afin de déverrouiller l'iPhone 5c de Syed Rizwan Farook, en occurrence fournir un logiciel permettant de contourner l'effacement automatique des données après dix tentatives infructueuses de saisie du mot de passe.

Depuis l'attaque du 2 décembre 2015, Apple et le gouvernement américain n'ont pas réussi à trouver un terrain d'entente. A la suite de la mise en demeure du juge, Apple s'est donc trouvée dans l'obligation de réagir. Le lendemain, Tim Cook, PDG d'Apple, a envoyé un message à tous les propriétaires d'iPhone annonçant un risque de surveillance généralisée des Américains si le FBI disposait d'un tel logiciel, appelant également « porte d'acier ». Il s'agit en fait de créer ou réparer une faille du système d'exploitation permettant d'accéder aux contenus protégés, une technique massivement utilisée par la NSA et rendue publique par les révélations d'Edward Snowden.

Pour Tim Cook, donner de tels moyens au FBI reviendrait à nier les libertés individuelles de ses utilisateurs, le ton étant alarmiste et rappelant les inquiétudes multiples ayant surgi à l'occasion de l'affaire Snowden : « Le gouvernement pourrait intercepter vos messages, regarder vos comptes bancaires et vos bilans de santé, et même accéder au micro et à la caméra de votre téléphone, sans que vous le sachiez.

 Â»

Aux Etats-Unis le débat est d'actualité très vif entre défenseurs des libertés individuelles et sécurité des citoyens

Deux jours plus tard, le 19 février 2016, le département américain de la justice déposait un recours pour obliger Apple à donner suite à la demande de la juge californienne avant le 26 février 2016. Apple n'a pas donné suite et a envoyé ses avocats défendre ses positions, ces derniers jugeant la demande «*contraire à la Constitution*», notamment du point de vue de la liberté d'expression si tant est qu'il s'agit de lignes de code relatives de la liberté d'expression.

Dans ce cas, la liberté d'expression peut aussi signifier le droit de ne pas s'exprimer. Au-delà des grands principes, la liberté d'expression étant inscrite dans le premier amendement à la Constitution américaine, Apple a contesté la base légale de la demande qui s'appuyait sur le All Writs Act. Cette loi de 1789 autorise les cours fédérales à assigner des personnes tierces à exécuter des demandes quand le Congrès n'a pas statué auparavant sur le sujet, à savoir dans tous les cas de *vide juridique*.

Hormis l'argumentaire juridique, la demande du FBI constituerait en fait pour Apple un précédent dangereux : en exigeant un logiciel permettant de passer outre les dispositifs de sécurité d'un iPhone, tous les utilisateurs seraient potentiellement concernés. Or, si l'enquête du FBI est légitime, la même demande pourrait être formulée par les gouvernements d'autres pays où Apple est présent, pays où le cryptage des données des utilisateurs a de fortes chances de ne pas servir exclusivement à la lutte contre le terrorisme.

Le sujet est délicat, alors même qu'aux Etats-Unis le débat est d'actualité très vif entre défenseurs des libertés individuelles et sécurité des citoyens, les deux étant essentiels à toute démocratie, mais la défense d'une liberté pouvant conduire à limiter l'autre, et inversement. Ce débat est notamment au cœur des enjeux politiques depuis les attentats de septembre 2001 et le vote du Patriot Act en octobre 2001.

La question posée par le conflit opposant l'Etat américain à Apple est celle de la légitimité des souverainetés économiques face au politique

Sur le plan économique, Apple a également beaucoup à perdre s'il devait être contraint de fournir les moyens de crypter le contenu des iPhone, puisqu'il ne serait alors plus en mesure de garantir à ses utilisateurs la confidentialité de leurs données. Dans une tribune publiée dans Les Echos du 1^{er} mars 2016, Gilles Babinet et Fabrice Epelboin considèrent que «*l'enjeu premier pour Apple n'est pas de protéger nos libertés, mais son image, sa souveraineté sur son cyber-territoire*

À», rappelant au passage qu'Apple n'a pas hésité à démanteler les données privées de ses clients chinois dans un data center géré par China Telecom à l'été 2015.

Le jugement est peut-être excessif, les dirigeants d'entreprise américaine cherchant bien sûr à protéger leur métier, mais aussi à ce qu'il est légitime de le supposer à les valeurs démocratiques de la société où ils sont nés et ont grandi. La protection de la vie privée en fait partie, même si elle a aussi une dimension stratégique du point de vue commercial avec tous les enjeux liés à l'exploitation des données personnelles.

Plus fondamentalement, la question posée par le conflit opposant l'État américain à Apple est celle de la légitimité des souverainetés économiques face au politique. Le cyber-territoire d'Apple, constitué de sa base d'utilisateurs, peut-il être véritablement inviolable, y compris par les services de renseignement de l'État où l'entreprise a son siège social ? Il s'agit dans cette affaire d'un cas grave de terrorisme. Il pourrait aussi s'agir d'un cas grave de sécurité publique. Ou de cas graves, mais moins sensibles pour la sécurité nationale, liés à des actes de délinquance.

La vraie question est donc de savoir où passe la ligne de séparation entre protection absolue des données personnelles et de la vie privée d'une part, et motifs supérieurs autorisant à revenir en partie et dans des cas exceptionnels sur le respect strict des libertés individuelles d'autre part. Le conflit d'Apple avec le FBI aurait pu être, de ce point de vue, l'occasion de statuer sur une doctrine partagée. Ainsi, le 1er mars 2016, un juge new-yorkais a refusé une requête des services de police dans une affaire de trafic de drogue, les enquêteurs demandant le déverrouillage d'un iPhone et s'appuyant encore à cette occasion sur le All Writs Act.

Le juge new-yorkais a pris soin de ne pas se prononcer sur la légitimité sur le fond de la demande mais a refusé de donner suite considérant que le All Writs Act a été conçu pour répondre à des vides juridiques constatés à la fin du XIX^e siècle, vides qui ne sauraient être de la même nature que ceux posés par la question du déverrouillage des smartphones. Un accord politique est donc nécessaire, ce qu'Apple rappelle le président des États-Unis, Barack Obama, le 9 mars 2016, à l'occasion d'une intervention au festival South by Southwest.

Après avoir rappelé qu'« un chiffrement solide [à l'ère] fétichise nos téléphones en les plaçant au-dessus de toute autre valeur », le président américain a laissé entendre que la défense exacerbée du droit à la vie privée va « à l'encontre de l'équilibre (entre respect de la vie privée et sécurité) que notre pays a atteint depuis deux cents ou trois cents ans », nécessitant donc de se mettre d'accord sur les cas pour lesquels le déverrouillage doit être imposé. Il reste que la chose est difficile à faire : fouiller une maison ne conduit pas à menacer l'intimité des foyers américains dans leur ensemble ; disposer d'un logiciel de type « porte d'entrée » permet techniquement de fouiller tous les smartphones, même s'il a été conçu pour répondre à un cas précis.

Dans cette affaire, les Etats-Unis n'auront malheureusement pas été en mesure d'apporter une réponse. Le 21 mars 2016, le FBI annonçait qu'un intervenant tiers lui avait montré une méthode permettant de débloquer l'iPhone 5c de Syed Rizwan Farook, un déblocage confirmé le 28 mars 2016, ce qui a mis fin aux poursuites contre Apple. Le FBI a en outre indiqué que l'entité ayant permis cet exploit n'était pas une agence américaine, ce qui revient à dire qu'il s'agit très probablement d'un organisme privé spécialisé dans la cybersécurité. Si tel est bien le cas, la souveraineté d'Apple a été mise à mal, l'affaire ayant révélé que ses iPhone ne sont finalement pas tous inviolables ; mais le pouvoir des agences américaines a également été ébranlé.

En effet, le FBI a été obligé de compter sur des acteurs économiques tiers pour parvenir à ses fins, une société israélienne collaborant d'ailleurs avec le FBI ayant été citée dans la presse. Ici, le politique, l'Etat et ses agences sont à chaque fois dépassés par les organismes privés qui mettent en place des dispositifs de protection de leurs clients, et mettent en place aussi les moyens de les contourner. La résistance d'Apple aux injonctions du gouvernement américain peut, de ce point de vue, être interprétée aussi comme une invitation faite aux hackers du monde entier à se spécialiser dans le déblocage des iPhone afin de revendre chèrement cette expertise aux agences nationales de sécurité, ou à Apple qui cherchera toujours à réparer les failles constatées dans ses systèmes d'exploitation.

A cet égard, l'administration Obama a demandé à ses agences de transmettre aux éditeurs informatiques les failles qu'elles découvrent dans leurs logiciels afin de mieux lutter contre la cybercriminalité. Cette règle souffre toutefois de quelques exceptions, notamment quand il s'agit de la sécurité nationale : le FBI n'a donc pas l'obligation formelle de donner à Apple l'information qui permettra au groupe informatique de renforcer son système d'exploitation.

Categorie

1. Articles & chroniques

date créée

29 août 2016

Auteur

alexandrejoux