Lettre n°53-Août 2016-disponible sur omc.ceis.eu

Brève du mois

« These evaluations are for supervising and guaranteeing that the security of this data accords with China's security standards. As for the legal requirement for internet operators to provide relevant data in the course of enforcement agencies' counter-terrorism and criminal investigations, this is necessary for safeguarding national security and investigating crimes. All countries do this. » Communiqué du Ministère des Affaires Etrangères chinois, en réponse aux groupes d'entreprises internationales exhortant la Chine de revoir son projet de loi cyber prévoyant des prérogatives d'audits de sécurité invasifs, ainsi que l'obligation d'héberger les données sur le sol chinois.

Table des matières

Y A-T-IL UNE VIE APRES LES GAFA ?

Google, Apple, Facebook et Amazon, les géants du numérique connus sous le nom de « GAFA », ou « les Big Four », dominent les marchés mondiaux. Google représenterait 91% de la recherche sur Internet, Apple 45% du trafic internet sur smartphone, Facebook 75% des réseaux sociaux et Amazon 6% de la vente en ligne[1]. Véritables puissances économiques, les GAFA et leurs 316 milliards de dollars de revenu annuel en 2013 génèrent autant de revenu qu'un pays comme le Danemark, et dépassent les 9% de croissance de la Chine en 2013 avec 13% la même année. Profitant de la transition numérique, ils investissent sans cesse de nouveaux marchés comme la santé, la médecine, l'automobile, les transports, l'énergie ou l'agriculture. Leur poids leur confère ainsi un véritable pouvoir d'influence politique et économique à l'échelle mondiale.

Un succès indiscutable qui n'est cependant plus incontesté puisque des voix de plus en plus critiques s'élèvent contre la toute-puissance des GAFA et certaines de leurs pratiques, notamment l'exploitation des données personnelles de leurs clients. La domination des GAFA sur les marchés mondiaux pourrait également être remise en cause par la monté en puissance des NATU (Netflix, Airbnb, Tesla, Uber), la génération montante des « disrupteurs » de la transformation digitale. Il n'est pas donc certain que la recette qui a longtemps fait le succès des GAFA leur permette de s'imposer dans la durée. Critiqués par les mêmes utilisateurs qui leur ont permis de bâtir et maintenir leur position dominante et rattrapés par la nouvelle vague de la révolution numérique, les GAFA sont-ils voués à s'incliner et à céder leur place ?

Les GAFA, un business model novateur clé d'une réussite fulgurante

Le client, un « utilisateur » créateur de valeur.

La spécificité et la force des GAFA résident d'abord dans un modèle économique novateur et original qui accorde une place centrale au client plutôt qu'au produit. Mais contrairement aux approches traditionnelles, le client des GAFA n'est pas « celui qui paye » car la plupart des services de ces quatre géants, du moins dans leur format d'appel, sont gratuits ou peu chers. Le client des GAFA se défini plutôt par l'attention qu'il porte aux services qui lui sont proposés, car il s'agit pour les GAFA d'attirer puis de retenir l'attention de l'utilisateur en optimisant l'« expérience » de celui-ci sur ses plateformes, afin de transformer son attention en engagement, et son engagement en revenu[2]. Car en utilisant les services gratuits qui lui sont proposés, le client partage des données et informations qui permettent de le cerner, de le comprendre, d'identifier ses habitudes et ses envies, et de lui faire au moment opportun des propositions commerciales qui y correspondent et qui l'intéressent, et qui sont créatrices de revenu. C'est donc l'utilisateur, non l'opérateur, qui crée de la valeur. Le client n'est plus défini comme « celui qui paye » mais comme « celui qui clique ».

Le Big Data, matière première des Big Four

La donnée se voit donc propulsée au cœur d'un système qui se nourrit des informations que les utilisateurs peuvent lui communiquer ou qui sont collectées, et qui sont agrégées et exploitées pour innover, proposer

[1] *GAFAnomics, New Economy, New Rules*, 2014

[2] *Gafanomics, les nouvelles règles du business qu'imposent Google, Apple, Facebook et Amazon*, Emmanuel Delsol, l'Usine Digitale, 26 Novembre 2014

de nouveaux services, et micro-cibler les internautes pour leur adresser une publicité personnalisée ou créer des produits susceptibles de les intéresser.

On distingue en fait deux modèles. D'une part Apple et Amazon, dont l'activité est articulée autour de la vente de produits et services, qui monétisent les données récoltées en proposant des services évolutifs payants type « Premium » ou en recommandant des produits matériels ou numériques à acheter en ligne ou dans leurs magasins. D'autre part Google et Facebook, qui exploitent les métadonnées ou utilisent les données issues des recherches commerciales de leurs utilisateurs pour leur proposer des produits ou services de partenaires commerciaux.

L'objectif des GAFA n'est plus tant d'être le moins cher mais de savoir proposer le bon produit au bon moment en fonction des besoins du client, besoins calculés par leurs algorithmes à partir des traces laissées par les passages et opérations de leurs clients sur leurs plateformes. La valeur des GAFA se mesure d'ailleurs au nombre de leurs utilisateurs plus qu'à la qualité de leurs produits, et tout l'enjeu est de réussir à établir avec le plus grand nombre d'utilisateurs une relation privilégiée. Car en maximisant l'expérience des utilisateurs les entreprises du digital en font aussi leurs meilleurs ambassadeurs, comptant sur le bouche-à-oreille pour assurer la promotion de leurs services et s'éviter ainsi des campagnes publicitaires coûteuses.

Les NATU : quand l'élève dépasse le maître

La réussite des NATU se manifeste par une progression ultra-rapide : Uber, par exemple, start-up fondée en 2009, pèse aujourd'hui plus de 62 milliards de dollars, contre 50 milliards seulement en 2015. Il a même déjà réussi là où les GAFA (à l'exception d'Apple) ont échoué, en s'imposant en Chine et en Inde.

Les NATU ou le règne de la plateforme.

Les NATU ne s'inspirent du modèle économique des GAFA que pour mieux le dépasser en en proposant une version encore plus radicale basée sur ce que Sangeet Paul Choudary qualifie de « plateforme biface » [3]. D'un côté les utilisateurs-producteurs qui créent la valeur (les propriétaires pour Airbnb ou les chauffeurs pour Uber), de l'autre les utilisateurs-consommateurs qui l'achètent. La valeur est donc non seulement créée mais aussi consommée par les utilisateurs. C'est la plateforme, plus que la technologie elle-même, qui constitue l'avantage comparatif des NATU et qui est au centre de leur modèle. Les services étant proposés par les utilisateurs eux-mêmes, ils ne supposent aucun investissement matériel de la part de ces entreprises : pas de voitures pour Uber ou d'hôtels pour Airbnb. Là aussi la valeur des plateformes augmente avec le nombre d'utilisateurs, et le système s'autoalimente sans que son développement et sa promotion ne nécessite d'investissement supplémentaire puisque ce sont les utilisateurs qui créent l'offre, qui l'entretiennent par le bouche-à-oreille, et qui l'enrichissent grâce à des services de parrainage.

3 Les NATU ou la conquête par la disruption, François Galtier et Hugo Breitwiller, pour Keley Consulting, 27 Novembre 2015

Les NATU ou le culte de la donnée

Autre domaine dans lequel les NATU dépassent leurs aînés : l'utilisation des données fournies, volontairement ou non, par les utilisateurs. Netflix est des NATU celui qui a de la façon la plus manifeste exploité la donnée à des fins de ciblage comportemental, et surpassé les GAFA dans l'utilisation et l'instrumentalisation des données. Dès 2009, le Prix Netflix, destiné à améliorer le service de recommandations de films de la firme, a récompensé les auteurs d'un algorithme permettant de prédire plus précisément les choix des utilisateurs dans leurs sélections de films. Les GAFA se contentaient d'utiliser les données collectées pour identifier des produits intéressants pour leurs clients ou améliorer les produits existants en fonction de leurs préférences. Netflix pousse la démarche encore plus loin pour concevoir des produits en fonction des prédictions sur les choix et préférences de films de ses consommateurs, prédictions établies par ses algorithmes à partir des comportements des utilisateurs sur sa plateforme. C'est le cas de la série House of Cards, réalisée sur la base des préférences des utilisateurs pour les acteurs, le réalisateur, la version britannique originale...[4]

Le digital au centre des usages

L'autre innovation majeure des NATU, c'est d'avoir su placer le digital au centre des usages. Ils proposent en effet une approche centrée sur leurs fameuses plateformes, véritables places de marché en temps réel auxquelles on accède d'abord et surtout par des applications mobiles. Les NATU ont ainsi « transform[é] l'économie du monde réel quand leurs ancêtres, les GAFA, étaient plus enclins à créer de la valeur et des services dans un monde virtuel et numérique[5] », et ont su profiter de la tendance grandissante à la « digitalisation » des usage autant qu'ils l'accompagnent et la facilitent.

Toutefois, la puissance relative des NATU n'est pas encore de nature à faire trembler les Big Four qui bénéficient d'une solide avance. L'arrivée de nouveaux « disrupteurs » portés par la multiplication des usages, notamment dans la FinTech, pourrait venir concurrencer les NATU. Certains marchés qui pouvaient sembler acquis aux NATU ont aussi vu l'apparition de sociétés locales concurrentes, comme Didi, concurrent chinois d'Uber valorisé autour de 28 millions de dollars.

Une concurrence féroce venue de l'étranger.

Des alternatives nationales en plein développement

La principale concurrence pour les GAFA vient de Chine et de Russie. En Chine, les BATX (Baidu, Alibaba, Tencent et Xiaomi) cumulent une capitalisation boursière impressionnante, un chiffre d'affaires en constante augmentation, une croissance plus que rapide et un développement exponentiel sur les marchés nationaux et régionaux, autant de signes d'une réussite insolente. Baidu, le Google chinois, s'est imposé comme le quatrième site internet le plus visité au monde, alors que les plateformes du géant du e-commerce Alibaba totalisent plus de 420 millions de clients. Tencent gère les services internet les plus populaires en Chine qui combinent ceux proposées par les américains Whatsapp, Apple Pay, ou Google Actualités, et Xiaomi,

4 Giving Viewers What They Want, David Car, The New York Times, 24 Février 2013

5 Transformation Numérique – 13 : GAFA vs TUNA – La guerre des maîtres du monde ?, 23 Février 2016

l'Apple asiatique, est à ce jour la 2ème start-up la plus valorisée au monde après Uber. A leurs côtés, Didi, le service de VTC le plus populaire en Chine comptabilise 300 millions d'utilisateurs.[6] En Russie, les concurrents les plus solides sont Yandex, le moteur de recherche qui fait de l'ombre à Google, Vkontakt, l'alternative russe à Facebook, entrée en 2014 dans le top 10 des réseaux sociaux avec 228 millions d'utilisateurs,[7] ou encore Telegram. Comme les GAFA, leurs homologues étrangers ont rapidement compris qu'il leur fallait se diversifier pour se développer et les BATX notamment ont développé des systèmes de paiement propres, des applications de mapping, et pour certains des organismes de crédit pour TPE ou un groupe de télévision et de production.

Les raisons de ce succès tiennent à la fois à la spécificité de leurs marchés intérieurs et à des politiques en matière d'économie numérique qui encadrent de très près les marchés pour favoriser les entreprises chinoises au détriment des sociétés étrangères. Dans cet environnement hostile aux GAFA, les BATX et leurs pairs russes se positionnent comme de véritables champions nationaux. Une position qui permet au BATX de se développer en Asie du Sud-Est, principalement à Singapour et dans les pays émergents, des marchés encore largement fermés aux firmes américaines. Certains viennent même concurrencer les Etats-Unis sur leur propre continent, comme Baidu au Brésil avec ou Tencent en Amérique du Sud, et même aux Etats-Unis, ou Baidu a créé un laboratoire dans la Sillicon Valley, ou en Europe, où il a investi massivement dans l'application finlandaise de géolocalisation de smartphones Indooratlas. Une réussite manifeste qui ne préjuge pas pour autant d'un succès sur le long terme. S'ils s'imposent sur les marchés nationaux, l'international ne représentent encore qu'une infime partie de leur chiffre d'affaires : 7% pour Tencent ou 10% Alibaba. D'autre part, ils font face, sur les marchés étrangers, à des entreprises bien établies sur lesquelles il n'ont pas forcément l'avantage. Pour conquérir d'autres marchés, les géants chinois du numérique devront également adapter leur marketing à des consommateurs aux profils et aux besoins différents, et se débarrasser d'une réputation entachée par des soupçons de contrefaçon et d'espionnage industriel. Quant aux plateformes russes, Vkontake et Telegram se sont attirés les foudres des autorités[8] et Vkontake a dès 2013 été placé sur "liste noire," se voyant ainsi retirée l'autorisation de distribuer des contenus en Russie.

D'autre part, même si Yandex s'est démarqué de Google avec un navigateur qui protège les données personnelles, les géants du numérique, quelle que soit leur nationalité, font l'objet de critiques répétées qui pourraient remettre en cause leur domination.[9]

Des pratiques discutables de plus en plus contestées

A bien des égards, la réussite des GAFA et des NATU s'est construite au détriment des individus-utilisateurs dont les données personnelles sont stockées et réutilisées sans leur consentement. La puissance économique et le pouvoir d'influence des GAFA et bientôt peut être des NATU n'est pas non plus sans inquiéter d'autres puissances établies, les Etats, qui se voient concurrencés dans leurs prérogatives souveraines.

6 Baidu, Alibaba, Tencent et Xiaomi : ces incroyables « GAFA » chinois, Capital, 18 juin 2016.

7 Russie, VKontakte placé sur liste noire, Le Figaro, 25 mai 2015

8 idem

9 Le russe Yandex défie Google avec un navigateur qui protège les données, Jamal al Hassani, Le Figaro, 26 mai 2015

GAFA et NATU, les nouveaux Big Brothers

La course à la donnée personnelle, carburant du modèle économique des GAFA, les pousse à des pratiques contestées en matière de protection de la vie privée. Si les législations commencent à s'adapter et à réagir, les flux de données sont encore très peu contrôlés, laissant une liberté considérable aux GAFA et à leurs successeurs dans l'utilisation de ces informations parfois personnelles. Les révélations sur ces pratiques discutables se succèdent : exploitation par Facebook et Google des données de navigation à des fins publicitaires, tentative de Facebook de s'attribuer la propriété commerciale des photos postées sur Instagram en changeant les conditions d'utilisation de l'application, marquage des images par des logiciels de reconnaissance faciale… Les individus, dans ce modèle, sont devenus « des produits en échange de services a priori gratuits »[10], les européens étant ainsi devenus les premiers exportateurs de vie privée[11]. Or l'utilisateur, ainsi conçu comme un client et un consommateur avant d'être un individu, accepte de moins en moins ce nouveau statut. Ces pratiques ont d'ailleurs un impact direct sur l'image et la réputation de ces sociétés : selon l'étude Fabernovel, seuls 41% des Français estiment que ces marques doivent être des exemples à suivre pour les entreprises traditionnelles.

Face aux GAFA et NATU, des Etats diminués

Ces plateformes défient aussi les Etats dans ce qu'ils ont de plus précieux, leur souveraineté, tant sur le plan politique qu'économique. Car les données collectées par ces sociétés d'envergure mondiale mais domiciliées aux Etats-Unis, donc américaines, leur appartiennent. Une situation qui consacre l'extra-territorialité de la législation américaine, puisque si les data centers installés hors des Etats-Unis sont protégés et jalousement maintenus hors de portée de ces Etats, ils sont ouverts aux agences fédérales et au système judiciaire américain.

Le contrôle des réseaux et des données qu'ils génèrent reste donc entre les mains de ces GAFA, et la France, comme les autres pays européens, est en matière de réseaux « sous tutelle étrangère »[12]. Une situation de fait qui n'est pas sans causer de vives tensions entre les Etats-Unis et les Etats européens. Les points d'achoppement sont multiples mais toujours à la fois pratiques et symboliques : le contrôle des Etats sur les informations sur leurs administrés, leur capacité à mettre en œuvre leurs politiques de lutte contre le crime et le terrorisme, et le prélèvement des impôts. Autant de prérogatives régaliennes pour lesquelles les Etats se voient privés de leurs capacités d'action, ce qui n'est pas sans conséquence sur leur efficacité et qui représente un manque à gagner non négligeable : selon le Boston Consulting Group, la valeur des données personnelles fournies par les Européens pourrait atteindre 1 000 milliards d'euros en 2020.[13] Grâce à des techniques d'optimisation fiscale, les GAFA réussissent en effet à ne reverser qu'une partie de leurs revenus aux Etats : 7 millions pour Apple, qui passe par le Luxembourg, l'Irlande et les îles britanniques, 3,3 millions pour Amazon, dont les fonds transitent par le Luxembourg, le Delaware et Gibraltar, ou encore 5 millions pour Google[14].

10 Vous avez aimé les GAFA, vous adorerez les NATU, Edouard Laugier, Le Nouvel Economiste, 28 Octobre 2015

11 idem

12 La souveraineté Numérique, ce dossier qui effraie Hollande et Valls, Emmanuel Berretta, Le Point, 13 janvier 2016

13 Vos données personnelles valent 315 milliards d'euros, Pierre Fontaine, 01Net, 12 novembre 2012

14 La ruée vers l'or des données personnelles, Claude Vincent Les Echos, 7 mars 2013

C'est cette question de la taxation qui a servi de point de départ à une contre-offensive menée par les Etats européens et qui a pour but de rééquilibrer leurs relations avec les GAFA à plusieurs niveaux, à la fois entre l'Europe et les Etats-Unis mais aussi entre la puissance publique et les firmes multinationales, et de créer, à terme, un environnement dans lequel les GAFAs ne seraient plus les maîtres des marchés du numérique et de la donnée personnelle.

L'individu contre-attaque

Si l'individu ne dispose encore d'aucun moyen légal ou formel pour s'opposer aux pratiques des Big Four, la dépendance de leurs modèles économiques à la satisfaction de leurs utilisateurs les contraindront à adapter même à la marge certains services en fonction du degré de tolérance de leurs clients à leurs pratiques intrusives. D'où le rôle des « lanceurs d'alertes », qui mettent à jour les abus des GAFA pour provoquer parmi leurs utilisateurs un désaccord suffisant pour faire pression sur ces sociétés et les forcer à revenir sur certaines pratiques. Un combat dont ils ne sortent pas toujours vainqueurs, comme le montrent les affaires Snowden ou Schrems, mais qui pourrait éroder la toute-puissance de ces sociétés. Face à la méfiance grandissante des utilisateurs, certains ont d'ailleurs dû accepter de reculer et de mettre fin à certaines pratiques pour les satisfaire. C'est le cas par exemple de Facebook, contraint de fermer son service publicitaire Beacon[15].

De leur côté, les autorités sont également plus vigilantes et prennent conscience de la nécessité d'adapter la législation aux exigences de protection des données personnelles pour permettre aux individus de faire valoir leurs droits : Google a ainsi été contraint par la CNIL à annoncer sa condamnation à une amende 150.000 euros pour « manquements à la loi informatique et libertés » pendant quarante-huit heures sur la page d'accueil de Google France en 2013, alors qu'Amazon et Apple ont été accusées d'« optimisation fiscale » par la Commission européenne. Des mesures qui ne sont certes pas en mesure de porter atteinte à leur toute puissance, mais qui marque une volonté grandissante pour les Etats de se placer en protecteurs de la vie privée des utilisateurs face à ces firmes.

Le retour de l'Etat souverain

Puisque les données personnelles sont au cœur des modèles économiques des GAFA et leur monétisation la principale source de revenu de ces sociétés, c'est en remettant en cause l'emprise de ces sociétés sur les données et l'utilisation qu'elles en font que les Etats européens, notamment par la voix des institutions européennes, entendent réaffirmer leur autorité. Depuis la mise en place de la nouvelle Commission en 2014 et sur la base des principes de la protection des données énoncés dans ce qui allait devenir en avril 2016 le Règlement européen sur la protection des données, l'Union européenne et ses Etats membres ont envoyé aux GAFA une série de signaux forts témoignant de leur volonté de s'imposer et de relocaliser l'application du droit. Dès 2014, la Commission a obtenu de Google l'établissement d'un « droit à l'oubli » qui permet aux citoyens européens d'exiger la destruction de certaines données personnelles les concernant. L'année suivante, plusieurs pays dont la France ont également ouvert une enquête sur la politique de confidentialité de Facebook, accusé d'avoir insuffisamment communiqué à ses utilisateurs les modalités de l'utilisation de leurs données. La Cour européenne de justice doit quant à elle se prononcer sur l'autorisation pour Facebook de transférer les informations sur ses clients européens Outre Atlantique. L'offensive est aussi venue de la Commissaire à la Concurrence qui a épinglé les Big Four pour leurs parts

[15] La ruée vers l'or des données personnelles, Claude Vincent Les Echos, 7 mars 2013

de marchés contraires à la législation européenne : accélération de l'enquête pour abus de position dominante contre Google, ouverture d'une enquête contre Android pour les mêmes griefs… Le niveau de sanctions prévu pour une société contrevenante a également été accru pour s'établir à 4% maximum du chiffre d'affaire.

C'est ensuite en matière de taxation que les Etats européens ont réagi, dans le but de forcer les GAFA à abandonner leurs pratiques fiscales discutables et à respecter la législation des pays dans lesquels ils opèrent. Alors qu'Apple fait toujours l'objet d'une enquête concernant de possibles accords fiscaux en Irlande, Amazon a du accepter de comptabiliser ses ventes dans les pays où il détient une filiale et de s'y acquitter des taxes sur les sociétés. La France a aussi tenté d'instaurer une "taxe Google" pour obliger la société à payer des impôts dans le pays et a poussé l'adoption par l'UE d'une directive qui l'oblige à s'acquitter de la TVA. Une version revisitée de la taxe carbone sur le modèle collecteur-payeur est également à l'étude.

L'émergence d'une stratégie européenne

Au-delà des tentatives de minimiser l'emprise des GAFA, il s'agit pour les Etats européens de faire émerger, pour contrebalancer la puissance des Big Four et de leurs cadets, un géant européen du numérique qui devrait permettre aux Européens de réaffirmer leur « souveraineté numérique ». C'est l'objet même du projet de « Marché unique du numérique » qui se présente comme un « cadre réglementaire assurant une concurrence équitable entre les acteurs numériques »[16] et doit permettre de poser les premières pierres d'une politique industrielle du numérique.

Force est de constater que, mise à part le Suédois Spotify, n°1 mondial du secteur et fort de 40 millions d'utilisateurs, et le Français Deezer avec ses 65 millions d'euros de chiffre d'affaires, l'industrie Européenne enregistre un réel retard. D'abord, les entreprises européennes sont absentes à presque tous les niveaux de la filière industrielle, ce qui ne fait qu'accroître leur dépendance à l'industrie américaine[17]. Ensuite, un marché européen encore beaucoup trop fragmenté entre 28 entités réduit les sociétés européennes à des marchés encore trop étroits quand les sociétés américaines opèrent dans un marché unique et vaste. Sans compter l'absence de synergies au niveau national, un obstacle de plus aux fusions nécessaires à l'émergence de sociétés pan-Européennes[18].

Les causes de ce déséquilibre sont multiples. Parmi elles, une structure de financement non adaptée qui ne permet pas de soutenir et de faire grandir les start-ups, et un modèle de distribution des risques qui ne permet pas d'encourager la réussite des projets les plus prometteurs. « Concrètement », explique Sébastien Soriano, « on doit accepter que des entreprises puissent perdre massivement de l'argent pendant des années avant de trouver un modèle économique viable.»[19] Car Outre-Atlantique, "50 % des investissements ne rapportent rien ; 30 à 40 % ont un retour sur investissement proche de zéro ; entre 10 et 20 % contribuent

[16] Numérique, Comment la France souhaite changer l'Europe, Toute l'Europe, 25 juin 2015

[17] Vous avez aimé les GAFA, vous adorerez les NATU, Edouard Laugier, Le Nouvel Economiste, 28 Octobre 2015

[18] Time to deliver on the Digital Single Market, Tomasz Poręba, Euractiv, 23 mai 2016

[19] « L'Europe doit se doter d'une politique offensive vis-à-vis des géants du web » Interview de Sébastien Soriano par Pierre Manière et Sylvain Rolland, La Tribune, 21 mai 2015

à la rentabilité globale des fonds[20]. Si les initiatives nationales se multiplient (comme en France les 500 millions d'euros de BPI), elles sont encore loin d'être suffisantes pour permettre aux start-ups européennes de s'affirmer. Pour se mesurer aux géants américains du net et s'affranchir de leur « colonisation numérique »[21], les Européens doivent donc mettre en place rapidement une réglementation harmonisée et un environnement permettant de favoriser une concurrence saine entre les acteurs européens et américains.

Contraints par leurs utilisateurs de revoir un modèle qui a longtemps fait leur force, concurrencés par de nouvelles générations de « disrupteurs » du numérique et contestés par des Etats en quête de souveraineté, les GAFA devront donc accepter de revenir sur certaines de leurs pratiques et de relâcher au moins partiellement leur emprise sur les marchés internationaux. Si leurs successeurs ne sont pas encore en position de remettre en cause leur suprématie, l'arrivée de nouveaux acteurs audacieux pourrait à terme remettre en cause l'équilibre actuel. Les initiatives politiques et juridiques menées par l'UE et l'émergence d'alternatives industrielles à l'échelle européenne pourrait également, dans un futur plus ou moins proche, affaiblir les Big Four et redessiner le paysage industriel du numérique.

[20] Vous avez aimé les GAFA, vous adorerez les NATU, Edouard Laugier, Le Nouvel Economiste, 28 Octobre 2015

[21] Comment l'Europe veut mettre les GAFA au pas, Sylvain Rolland, La Tribune, 28/05/2015

LA SECURITE DES MOTS DE PASSE

Si l'actualité de la sécurité informatique traite beaucoup de vulnérabilités et de malwares, elle a tendance à nous faire oublier que la base de la sécurité informatique repose en grande partie sur l'authentification, et que celle-ci utilise principalement le mot de passe.

Afin de sécuriser nos mots de passe, nous avons appris à les complexifier. Mais ceci conduit parfois à une illusion de sécurité. Le *passcracking*[22], discipline qui a pour objectif la récupération par « brute force » des mots de passe, montre en effet que leur robustesse dépend beaucoup de la façon dont ils ont été générés.

Une illusion de sécurité

Afin de sécuriser nos mots de passe, nous avons appris à les complexifier : multiplier les caractères, utiliser à la fois des minuscules et des majuscules, inclure des chiffres et des caractères spéciaux, etc. Armé d'un tel mot de passe, il est tentant de considérer celui-ci comme étant suffisamment solide. En réalité, cette robustesse dépend beaucoup de la façon dont il a été généré.

Les bases de données contenant des mots de passe nous apprennent beaucoup sur la façon dont la majorité des utilisateurs créent leurs mots de passe… Des enseignements mis à profit par les *passcrackers*, qui ont ainsi pu définir des schémas courants, ou *patterns*, suivis par de très nombreux utilisateurs. Le problème se situe effectivement dans la tendance que nous avons à complexifier nos mots de passe de la même façon[23].

Ces *patterns* permettent d'augmenter grandement les chances de découvrir un mot de passe, en évitant de tester toutes les combinaisons possibles (technique du *bruteforce*). Ils permettent effectivement de générer des "candidats", qui seront automatiquement testés. Une règle pourra ainsi être de tester d'abord les mots de passe constitués d'un mot dont la première lettre est une majuscule, complétés d'un ou deux chiffres puis d'une ponctuation en toute fin de mot de passe.

Nous le verrons, qu'il s'agisse de *passcracking* hors-ligne ou en ligne, le *passcracker* a intérêt réduire au maximum le nombre de tentatives nécessaires à la découverte du mot de passe.

Passcracking : en ligne ou hors-ligne

En ligne, le *passcracking* consiste pour l'attaquant à tester des mots de passe directement sur un serveur légitime. Celui-ci possédera le plus souvent des mesures de protection. La première est de limiter le nombre de tentative d'identifications en fonction du compte ciblé ou de l'adresse IP de provenance des tentatives. Si du fait de ce type de mesures, le *passcracking* en ligne est généralement très limité, on ne peut cependant pas complètement l'exclure. Du fait de ces protections, un attaquant va en général pouvoir tester un mot de

[22] Le passcracking n'est légal que sous condition d'obtenir l'accord du propriétaire du système d'information considéré, généralement à des fins d'audit de celui-ci ou de recherche scientifique.

[23] Ceci est renforcé par les systèmes qui forcent les utilisateurs à respecter certaines règles pour la composition de leur mot de passe, ce qui incite finalement les utilisateurs à se conformer au strict minimum demandé, en suivant généralement un même schéma.

passe par minute en moyenne. En revanche, un serveur qui ferait l'impasse sur une protection par compte utilisateur permettrait au possesseur d'un botnet d'augmenter radicalement ses capacités.

Hors-ligne, le *passcracking* correspond à un travail sur des empreintes de mots de passe à partir d'une base de données volée. En effet, la pratique consiste à ne pas stocker les mots de passe eux-mêmes en base de données, mais de seulement y conserver leur empreinte, ou *hash*.

Une telle empreinte s'obtient en faisant passer un mot de passe à travers une fonction de hachage : il s'agit d'une fonction mathématique complexe qui fait correspondre à chaque mot de passe un résultat contenant un nombre fixe de caractères, quel que soit le mot de passe considéré. Lorsqu'un utilisateur tente de se connecter à un serveur, celui-ci calcule l'empreinte du mot de passe envoyé par l'utilisateur, qu'il compare à celle présente dans sa base de données. Si les deux empreintes correspondent, la connexion est acceptée.

Ce fonctionnement oblige le calcul de l'empreinte de chaque mot de passe que l'attaquant souhaite essayer. Ce calcul, trivial pour le serveur légitime qui ne doit l'effectuer qu'une fois par connexion utilisateur, constitue le véritable facteur limitant du *passcracking*. Cela impose au *passcracker* d'utiliser toutes les techniques à sa disposition afin de réduire le nombre de combinaisons à tester : règles de mots de passe, information sur l'utilisateur ciblé, etc.

D'après Hydraze, spécialiste français reconnu du *passcracking,* sur les dumps de base de données à disposition sur Internet, on peut généralement casser en temps raisonnable entre 30 et 80% des mots de passe, simplement en utilisant les règles de mutation/substitution[24].

Les outils à disposition des *passcrackers*

Les logiciels d'audit. De nombreux outils d'audit facilitent le passcracking. Des logiciels tels que Hydra ou Medusa permettent de s'adonner en toute illégalité au *passcracking* sur tous types de services web : sites web, service mail mais également protocoles d'administration. Hors-ligne, d'autres logiciels tels qu'Hashcat ou John The Ripper permettent d'automatiser le *passcracking* sur les dumps de bases de donnés.

Les « dictionnaires ». Afin de réduire le temps de recherche, on n'utilise pas la méthode de la force brute au sens strict du terme : on met en pratique de qui s'appelle l'attaque par dictionnaire. Il s'agit de fournir au logiciel une liste de mots de passe, laissant de côté les combinaisons purement aléatoires. S'il est facile de trouver ces dictionnaires en libre téléchargement, les plus efficaces sont bien entendu ceux qui sont constitués de mots de passe déjà cassés. Ceux-là sont évidemment plus difficile à obtenir, étant donné leur provenance généralement délictuelle…

Les tables arc-en-ciel, ou *rainbow tables*. Le premier facteur limitant du *passcracker* étant la puissance de calcul, il faut en limiter au maximum son besoin. Il s'agit donc de calculer une fois pour toutes les empreintes correspondant à une liste de mots de passe donnée, et de stocker le résultat au sein d'une table dite arc-en-ciel. La table pourra être utilisée dans toutes les tentatives futures, permettant un gain de temps considérable. Nous verrons qu'il existe des techniques pour contrer en partie l'usage des tables arc-en-ciel.

[24] http://www.comptoirsecu.fr/2016/05/episode-36-les-mots-de-passe/

Les mesures de protection : du côté de l'hébergeur

L'utilisation d'algorithmes appropriés. Toutes les fonctions de hachage ne sont pas faites pour le stockage de mots de passe. Certaines, comme SHA-1, ont été conçues pour permettre un calcul rapide de l'empreinte : une carte graphique de milieu de gamme est aujourd'hui capable de calculer plus d'une dizaine de milliards de combinaisons à la seconde[25]. Notons qu'il existe des algorithmes conçus spécifiquement pour être difficiles à opérer sur carte graphique. Cependant, les algorithmes recommandés aujourd'hui sont très minoritaires, et des algorithmes inadéquats continuent d'être fréquemment utilisés par des développeurs peu conscients des enjeux de sécurité.

L'application de plusieurs itérations de la fonction de hachage. Puisque l'avantage de la puissance de calcul est dans le camp de la défense, il est de bon ton de le renforcer en effectuant plusieurs boucles de l'algorithme de chiffrement.

L'usage de « sel » de chiffrement[26]. Le stockage des mots de passe s'effectue de la façon suivante : pour chaque utilisateur, quelques caractères aléatoires sont ajoutés au sein du mot de passe avant que ne soit calculé l'empreinte du résultat concaténé. Une ligne d'une telle base de données suit donc le modèle suivant :

id | identifiant | empreinte (mot de passe + sel) | sel

En cas de fuite de données, les sels sont également volés, mais cela empêche le hacker d'utiliser des tables arc-en-ciel et l'oblige à recalculer chacun de ses candidats de mot de passe avec chaque sel contenu dans la base de données. L'usage d'un sel de chiffrement permet de contrer l'usage par l'attaquant de tables arc-en-ciel. D'autre part, il oblige l'attaquant à recalculer l'empreinte de l'ensemble des mots de son dictionnaire pour tenir compte du sel correspondant à l'utilisateur.

L'emploi d'un « poivre » de chiffrement[27]. Celui-ci est unique, mais stocké au sein du code du logiciel ou du site web, et non dans la base de données. En effet, il arrive régulièrement qu'une base de données soit piratée sans que le serveur du site web ne le soit, et ce d'autant plus que les bases de données sont souvent hébergées sur un serveur distinct de celui du site à proprement parler.

La mise en place d'un système de double authentification. De plus en plus, il est proposé, voire imposé à l'utilisateur, un système de double authentification. En ligne, il s'agira souvent d'un code envoyé par mail ou par SMS que l'utilisateur devra saisir pour valider son authentification. Ce type de code peut également être généré par des jetons de sécurité physique[28].

La mise à disposition d'un indicateur de robustesse de mot de passe intelligent. Les indicateurs traditionnels de complexité des mots de passe, que l'on trouve depuis quelques années sur les formulaires de création de mot de passe de nombreux sites web, sont extrêmement basiques. Leur scoring ne s'attache

[25] Les passcrackers ont généralement recours aux cartes graphiques pour effectuer les calculs d'empreinte. Celles-ci étant optimisées pour la parallélisation des calculs, elles sont plus performantes que le processeur central.

[26] Le salage, est une méthode permettant de renforcer la sécurité des informations qui sont destinées à être hachées en y ajoutant une donnée supplémentaire afin d'empêcher que deux informations identiques conduisent à la même empreinte.

[27] Même principe que le salage, à ceci près que le « poivre » est stocké dans le code du logiciel et non dans la base de données.

[28] https://fr.wikipedia.org/wiki/Jeton_d%27authentification

en effet généralement qu'au nombre de caractères ainsi qu'aux typologies de caractères utilisés, et ne tiennent absolument pas compte des techniques employées par les *passcrackers*. Certains indicateurs évaluent plus sérieusement le scoring, comme ZXCVBN qui compare le mot de passe de l'utilisateur à sa liste des mots de passe les plus couramment utilisés, s'intéresse aux techniques de complexification habituelles, ou encore aux motifs géométriques du clavier tels que le *keywalking*[29].

Les mesures de protection : du côté de l'utilisateur

Les critères de protection

La meilleure façon pour l'utilisateur de se protéger du *passcracking* est de faire le choix :

- de mots de passe différents pour chaque service. Ceci à des fins de « damage control » afin que le piratage de l'un de ses comptes ne signifie pas le piratage de plusieurs de ses comptes. Les mots de passe ne doivent en aucun cas dériver les uns des autres, sans quoi des règles de substitutions et de transformation auraient vite fait d'en obtenir raison ;
- de mots de passe aléatoires. Ceux-ci mettent l'utilisateur à l'abris des biais cognitifs[30] rendant le mot de passe plus facile à deviner, pour une raison ou pour un autre. Tout ce qui contribue à rationaliser un mot de passe se retourne contre son créateur le jour où son mot de passe sera mis à l'épreuve d'un *passcracker* ;
- de mots de passe régulièrement renouvelés, ceux-ci pouvant être compromis à tout moment par la fuite d'une base de données. Il est important de noter que les utilisateurs de sites internet ne seront pas mis au courant de la plupart des piratages de bases de données, soit car les administrateurs décident de ne pas communiquer sur l'existence d'un piratage, soit que ceux-ci ne l'aient pas détecté. Les services tels que havelbeenpowned.com, qui permettent de vérifier que son compte ne figure pas parmi les fuites de bases de données disponibles publiquement, ne font qu'effleurer la surface d'un phénomène dont l'ampleur est difficile à appréhender.

Pour se conformer à ces différents critères, la meilleure (et peut être seule ?) alternative est de se tourner vers des logiciels de gestion de mots de passe.

Les gestionnaires de mots de passe

Un gestionnaire de mots de passe est un logiciel faisant office de porte-clés pour son utilisateur : il stocke au sein d'un même fichier chiffré ses différents mots de passe. L'utilisateur ne doit ainsi retenir qu'un seul mot de passe, le mot de passe-maître, avec lequel le porte-clés est chiffré. Celui-ci doit évidemment être aussi difficile à déterminer que possible. Il est donc conseillé d'utiliser non plus un « mot » de passe, mais une phrase complète, en continuant à faire appel à plusieurs jeux de caractères (alphanumériques, ponctuation, caractère spéciaux, etc.).

Un tel logiciel permet de s'affranchir des problématiques de mémorisation de nombreux mots de passe réellement complexes et régulièrement renouvelés. Certains de ces logiciels permettent d'ailleurs justement

[29] *Keywalking* : emploi de touches voisines en suivant une ligne (« azerty », « 123456 », ou justement « ZXCVBN »).

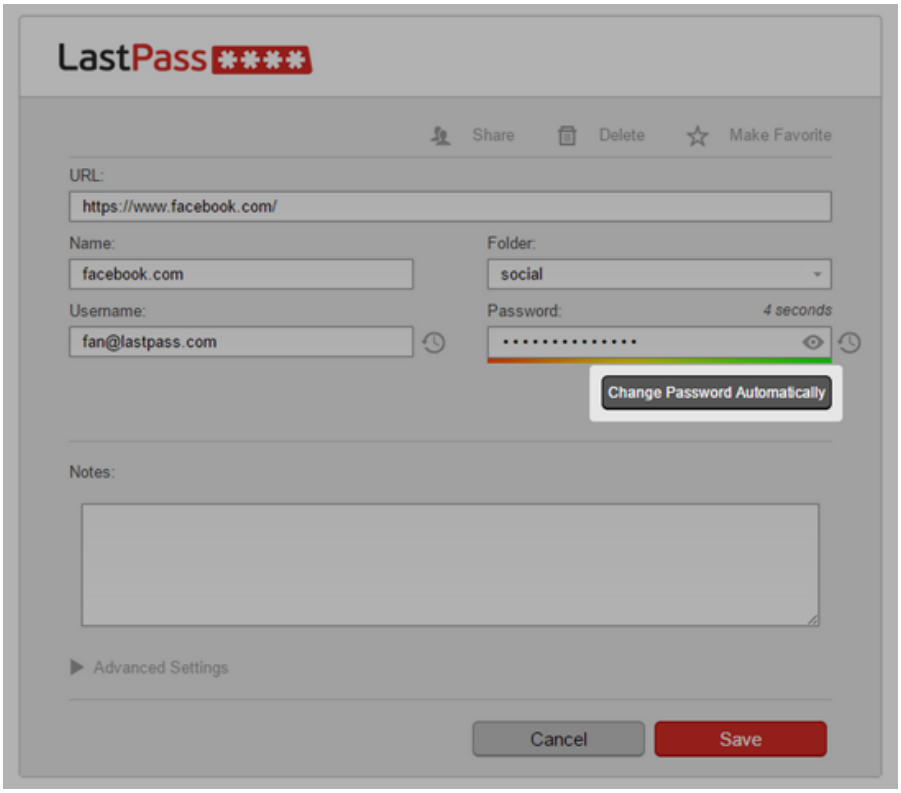
[30] Le piratage des bases de données de certains sites a mis en avant le fait que nombre d'utilisateur sont influencé par le contenu ou la charte graphique du site web considéré.

de procéder au changement automatisé des mots de passe de certains sites (ceux pour lesquels les développeurs ont adapté leur outil de gestion de mots de passe).

Il existe deux types de logiciels de gestion de mots de passe :

- Certains sont sous la responsabilité pleine et complète de l'utilisateur : la base de mots de passe est stockée sur l'ordinateur de l'utilisateur, ou tout autre support (clé USB notamment) souhaité. L'utilisateur est maître de son porte-clés, qu'il doit garder à disposition en cas d'utilisation nomade.
- D'autres, tels que Lastpass ou Dashlane, prennent la forme d'un service en ligne. Les mots de passe de l'utilisateur sont stockés dans le Cloud, toujours chiffrés avec le mot de passe-maître de l'utilisateur. L'intérêt de ce type de service réside dans le gain de temps offert à travers la synchronisation automatique sur l'ensemble des dispositifs informatiques de l'utilisateur (ordinateurs, smartphone, tablettes, etc.) et l'automatisation des procédures de connexion aux sites Internet (il n'y a pas besoin d'aller chercher manuellement chacun de ses mots de passe pour se connecter à tel ou tel service web).

Bien entendu, les logiciels de gestion de mot de passe génèrent leurs propres risques, qui se résument en grande partie à la question suivante : peut-on faire confiance à l'éditeur de la solution logicielle considérée ? Ces applications exacerbent en outre le risque engendré par une session utilisateur restée ouverte, ou associée à un mot de passe top faible (le mot de passe de session restant nécessairement à la charge de l'utilisateur).



Fonctionnalité de changement automatisé de mots de passe du gestionnaire de mot de passe Lastpass

La sécurisation de l'authentification repose sur de nombreux facteurs. Il est essentiel que l'utilisateur se donne les moyens de protéger ses accès. A lui de déterminer la meilleure façon d'y parvenir en fonction des risques identifiés.

Il est en outre de la responsabilité de chaque hébergeur de service de respecter l'état de l'art en matière de stockage des mots de passe (algorithme de chiffrement adéquat, utilisation de sel/poivre de chiffrement, etc.). A charge également pour eux de mettre à disposition des utilisateurs certains de ces moyens, notamment la double authentification.

Rappelons enfin que la sécurité des mots de passe de l'utilisateur est quoiqu'il en soit compromise dès lors que son poste est infecté par un malware. Celui-ci peut par exemple comporter un *keylogger* (en français : enregistreur de frappe) pouvant enregistrer tout mot de passe entré par l'utilisateur, y compris justement un mot de passe-maître. Cela ne signifie en aucun cas qu'il faille faire l'impasse sur la sécurité des mots de passe.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com