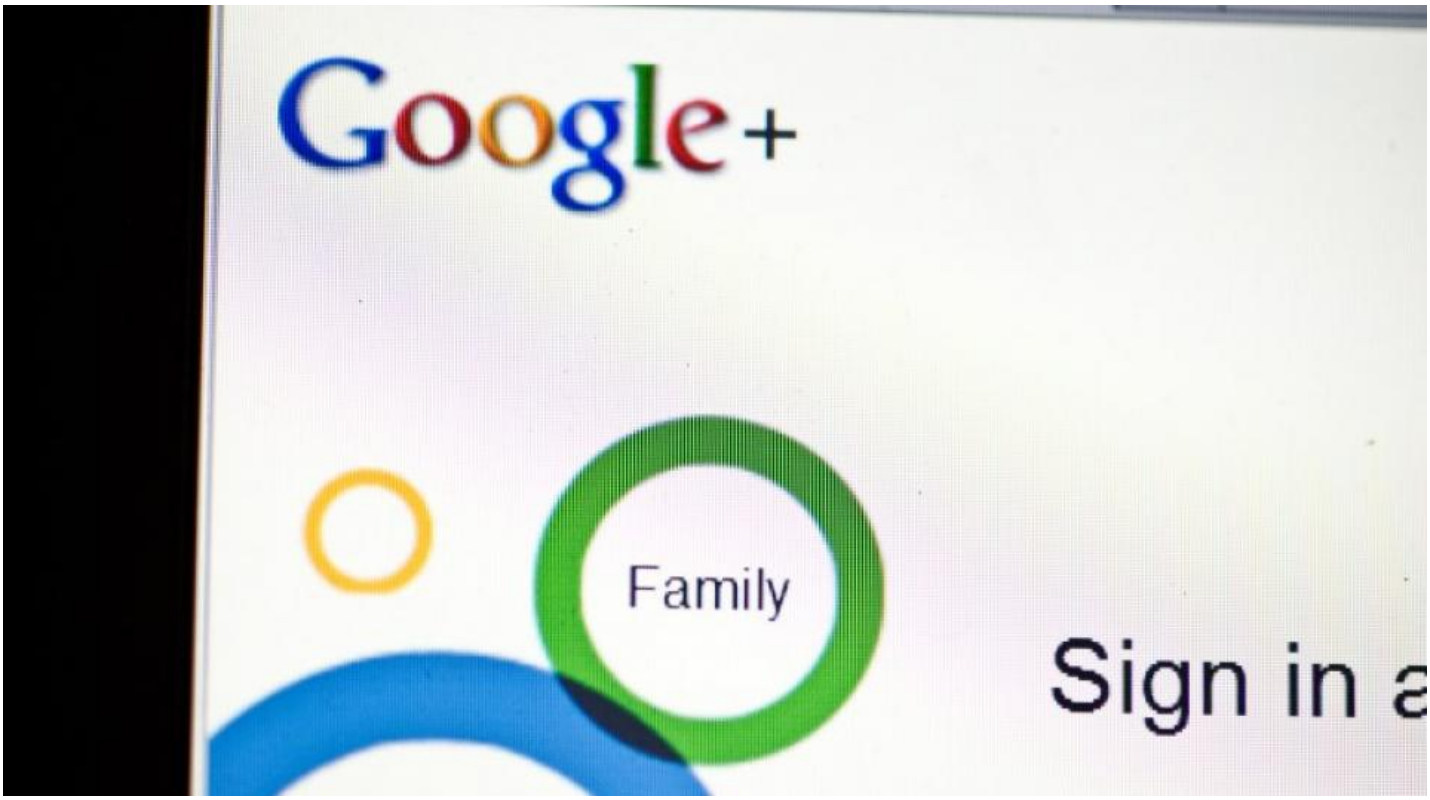
Mega failles de sécurité : peut-on raisonnablement faire confiance aux géants de la Tech pour protéger nos données ?



Ce lundi, le Wall Street Journal révélait qu'un bug au sein du réseau social Google + avait exposé au moins 500 000 comptes d'utilisateurs à la fuite de leurs données personnelles pendant deux à trois ans. Effrayé de l'outrage public suscité par le scandale Facebook-Cambridge Analytica, Google a fait en mars dernier le choix coupable de ne pas révéler cette faille technique.

Avec Eric Delcroix

Atlantico : Le bug de Google + n'a probablement pu toucher qu'un faible nombre de personnes en comparaison de la fuite massive opérée par Cambridge Analytica sur les données de près de 87 millions utilisateurs de Facebook. Peut-on néanmoins comparer le niveau de gravité de ces deux scandales ?

Eric Delcroix : Pour l'instant, on nous parle en effet de 500 000 comptes. Mais en réalité quand on regarde, on nous dit aussi qu'on ne dispose pas des données sur de très longues durées. De plus, l'estimation est faite par rapport au nombre d'applications tierces qui passent par l'API [interfaces de programmation], et pouvant potentiellement récupérer des données. Cela fait donc deux indicateurs que l'on peut manipuler différemment. Maintenant ce qui est vrai, c'est que si beaucoup de personnes se sont inscrites à une époque à Google +, aujourd'hui et depuis quelques années Google + est complètement mort. Par rapport à l'usage, je dirais donc que le chiffre correspond : plus grand monde ne s'y rend. Les données sont peut-être même très vieilles.

Le problème, pour Facebook comme pour Google, c'est l'ouverture des plateformes aux tiers. Ils confient l'accès aux API, que ce soit avec ou sans bug. Peut-être que ce qu'il s'est passé au niveau de Google, c'est simplement qu'il y a eu un changement de programmation quelque part dans Google qui a provoqué l'ouverture, c'est tout à fait possible. Les tiers, par la suite, on ne sait pas ce qu'ils font des données. La fuite est arrivée à Facebook et Google, mais cela peut arriver sur d'autres réseaux sociaux : LinkedIn risque tout autant, car il y a des applications tierces qui y viennent aussi.

Nous confions effectivement nos données à des sociétés comme Facebook et Google, mais on ne sait pas ce que les sociétés tierces vont faire avec. Tout le problème est là. Si on prend uniquement Facebook ou Google, alors oui on sait qu'ils prennent nos données, qu'ils les manipulent, ça oui. En revanche, la ligne rouge est dépassée lorsque les sociétés tierces arrivent là-dessus. Mais c'est un problème qui existe depuis longtemps : on avait des bases de données que l'on confiait à la Redoute ou aux Trois Suisses, on leur donnait régulièrement des informations et ils revendaient les fichiers. Mais que faisaient les gens qui avaient acheté les fichiers ? C'est exactement la même chose pour Facebook et Google.

En effet, une chose est de consentir à l'utilisation de nos données privées sur des plateformes comme Facebook, Apple ou Google, une autre de constater que ces données font l'objet d'un traitement industriel particulièrement oaque, parfois même illégal, de la part de leurs partenaires commerciaux. Dans un tel système à deux niveaux, quelle est la part de responsabilité de chacun des acteurs de ce

traitement ?

Il est dur de jeter la pierre aux GAFAs en considérant que c'est leur faute. Je pense que leur contrat sont sécurisés, le tout étant de savoir qui se retrouve dans les sociétés tierces, et quelle est la mentalité et l'usage qui en est fait. Il faudrait qu'ils aient un droit de regard sur ce qui est fait des données qui sont utilisés par les sociétés tierces. Ce qui devient compliqué. Parce qu'en retour, cela permet à Google ou Facebook (quoique Google n'ait plus de réseau social) de s'approprier un peu tout ce que font ces sociétés tierces. C'est ce que fait Google avec les sociétés de commerce. Quand il voit que vous vendez des choses qui sont intéressantes, avec des chiffres qui fonctionnent, il finit par prendre les produits pour les vendre lui-même. Là c'est la même chose, si le réseau social connaît les ventes que font les tiers avec ses données, il finit par s'y substituer. C'est toute la problématique que pose le fait d'encastrer les produits, où l'on peut mettre son œil dans les données des autres. Il est certes possible de faire des contrats, interdisant ou limitant certains usages, mais comment contrôler les intermédiaires derrière ? Ce qui se fait, c'est de prévenir les gens. Facebook prévient les gens qu'il n'émet que les données qui lui sont livrées directement. Si l'on passe par des sociétés ou des applications tierces, et il y en a quand même beaucoup, alors là, il n'est pas responsable car ce n'est pas lui qui le gère. Là encore, ce n'est pas neuf : on peut faire le parallèle avec les blogs où l'on retrouve le même problème. Il y avait eu des problèmes en France avec certains bloggeurs dont on se demandait s'ils étaient simples hébergeurs de l'information ou bien exploitant de l'information. Lorsqu'on met à disposition une plateforme de blog, et que des gens publient des conneries à l'intérieur, est-ce qu'on est responsable ? C'est un problème juridique par excellence.

La mise en œuvre en mai dernier du RGPD était appelée à accroître la protection des données des citoyens européens, peut-on déjà en mesurer les résultats ?

Le premier résultat que l'on voit en règle générale ne va pas dans le bon sens : quand je vois le nombre de personnes qui râlent parce que les Américains nous bloquent l'accès à leur site. C'est que ceux-là ne peuvent pas respecter la règle européenne, alors ils bloquent. Alors voilà, on a plus accès aux sites de cuisine américains parce qu'on est Européens. Au-delà de ça, personnellement je n'ai pas vu de changement. Tout le monde a fait un message en disant "attention, vous nous accordez bien le fait qu'on peut vous envoyer des mails" mais je n'ai rien vu d'autre. J'en avais déjà parlé dans Atlantico : de toute manière pour le grand public, cela ne changeait pas grand-chose.

Les entreprises essayent de se mettre à la norme, mais ce n'est pas parce qu'il y a une contrainte quelque part que les gens ne vont pas la dépasser ou la contourner à un moment ou à un autre. En ce qui concerne l'utilisateur final, dans le méandre de ce qui se passe, il est complètement à côté de la plaque, il ne voit rien du tout. D'autant que l'idée demeure forte que sur internet tout est libre.

Le renforcement du pouvoir des autorités régulatrices est-il une bonne solution ?

Au niveau du régulateur, il doit y avoir une constatation : tout ce qui se fait maintenant, en termes de procès, de procédures, contre les GAFAs, au niveau européen, etc., tout cela va accoucher d'une souris. Peut-être que ca peut marcher en Chine, mais ce n'est pas la même structure que chez nous.

Curieusement, je pense que le seul moyen dont on dispose, il faut le reconnaître à Facebook : c'est que dès qu'il y a un problème, on en parle. On voit la différence avec Google. Facebook dit ce qu'il se passe, et essaie de trouver des solutions. Et justement, concernant Google, j'ai souvent le sentiment inverse en me disant : attention, Google ne dit pas tout. Là, on en a la preuve. Il est certain qu'avoir des réseaux sociaux, avoir des données, les manipuler, tout cela suppose des dangers. Or je pense que Facebook est très conscient de ce qu'il se passe à son niveau et de ce qu'il a entre les mains. Bien sûr cela n'empêche pas les problèmes.

Un fossé est-il en train de se creuser sur ces questions entre Européens et Américains ?

Il y a une grande différence, qui est une différence culturelle. On le voit par exemple par rapport aux publications de photos. Les Américains publient leur image, et s'il y a un problème, ils retirent. Nous, Européens, en particulier au Sud, on réfléchit avant si l'on peut publier ou non. Je crois que l'on retrouve cela à tous les niveaux. Les Américains publient leurs données, et s'il y a un problème, ils les retirent. Chez nous, pour les publier, il faut que les données soient en sécurité. Je ne dis pas que telle ou telle solution est la meilleure, mais en tout cas, il y a là un fossé qui a toujours existé.