Snapchat gardait en fait vos photos censées être détruites : faut-il faire confiance à qui que ce soit sur le web ?

Snapchat, l'application d'envoi de photos destinées à disparaître en moins de 10 secondes, a été épinglé par les autorités américaines pour avoir laissé s'installer une faille de sécurité.

Avec Etienne Drouard

Atlantico : Le gendarme du web américain (la Federal Trade Commission) vient d'épingler l'application Snapchat, qui n'a pas rempli son engagement de faire disparaître les photos envoyées par son biais en moins de 10 secondes. Malgré les engagements des acteurs du web, on a l'impression que ce sont toujours de vains mots. Est-il possible de faire confiance à qui que ce soit sur le web ?

Etienne Drouard : On peut davantage faire confiance aux acteurs du web qui font l'objet d'un contrôle. En l'occurrence Snapchat n'a pas volontairement rompu sa promesse, mais était sous le contrôle de la Federal Trade Commission, qui à l'occasion d'une faille de sécurité des données a audité leur système, pour constater que la suppression des photos annoncée par l'entreprise n'avait pas un effet absolu si on utilisait certaine applications, qui elles, pouvaient maintenir la conservation. Le rapport de confiance est probablement plus légitime par conséquent lorsqu'un régulateur indépendant effectue des contrôles.

Dans le cas de Snapchat, comment expliquer que depuis sa création en 2011, l'application ait conservé une trace des photos, alors que par nature, son service consiste à les faire disparaître au bout de dix secondes ?

Ce "mensonge" n'est pas volontaire, la suppression des données a été effectivement programmée par Snapchat, mise en œuvre sur les serveurs de l'entreprise, mais elle n'empêchait pas des utilisateurs d'effectuer une copie en utilisant une fonctionnalité de transfert à un ami. Au travers de cette fonctionnalité, la suppression effectuée par Snapchat n'a pas d'effet. C'est une erreur de conception par Snapchat, qui fait croire à une information de courte durée, et a bêtement mis une fonctionnalité d'envoi de message électronique. Cela relève davantage de l'incompétence que du mensonge.

Faut-il en déduire comme loi intangible qu'il ne faut faire entièrement confiance à aucun service proposé sur le web ?

La loi intangible est la suivante : croire en ce qu'on nous dit ne suffit pas, il faut également que ceux qui affirment un certain niveau de protection de la vie privée s'astreignent ou soient astreints à des mécanismes d'audit. Autrement, les discours et les clauses contractuelles ne peuvent pas suffire pour garantir l'effectivité des engagements dont on croit bénéficier.

Qui sont les acteurs du web dignes de confiance ? En existe-t-il seulement ?

Deux régions du monde imposent un audit des entreprises par des auditeurs indépendants : les Etats-Unis et l'Union européenne. Les Etats-Unis obligent les entreprises à un audit lorsqu'une faille de sécurité survient (car elles sont obligées de la déclarer), et pour éviter ce type de faille, les entreprises s'auto auditent avec des indépendants. Ce n'est pas systématique, mais telle est la tendance. L'UE a mis en place un mécanisme comparable de révélation des failles de sécurité (c'est ce qui a amené Orange à en révéler une il y a une dizaine de jours), et un contrôle par un régulateur indépendant (la Cnil en France).

Les acteurs dignes de confiance sont ceux qui mettent carte sur table, et qui se dotent de mécanismes d'audit. Sinon, la confiance du consommateur repose sur la croyance dans une marque, et jusqu'à preuve du contraire ce n'est pas cela qui fait la sécurité informatique d'une donnée. Les entreprises qui savent qu'elles disparaîtront en cas de déficit de confiance s'obligent à s'exposer à des auditeurs externes. On a par exemple entendu parler de failles de sécurité chez Facebook au moment d'une migration de systèmes, ou sur les comptes Gmail. Même dans ces sociétés la fiabilité à 100 % n'existe pas. J'ajouterai que l'un des acteurs de la confiance est aussi l'utilisateur, qui ne doit pas attendre des entreprises qu'elles se comportent comme la Banque de France avec de l'argent.

A quelles exigences les services en ligne des banques sont-ils soumis, et sont-ils suffisants ?

Elles sont astreintes à des normes de sécurité qui leur sont imposées au regard de leur secteur d'activité, avec des cahiers des charges, des livres blancs, des normes internationales, pour fixer un standard minimum censé couvrir les risques. Chaque fois que ces standards sont dépassé, c'est soit par une intention malveillante, soit par une menace qui jusqu'à présent n'était pas identifiée par les acteurs, qui font sans cesse adopter de nouvelles normes.

Par exemple, les paiements par carte bancaire bénéficiaient d'une très grande sécurité grâce à la puce, mais celle-ci a fini par être violée il y a une quinzaine d'années. On a donc abouti à des régimes de couverture par les banques des failles de sécurité sur le moyen de paiement, et lorsque c'est devenu trop coûteux pour elles, on a élaboré la norme 3D Secure, qui consiste à ajouter au numéro de la carte bancaire un identifiant fourni par SMS.

On peut donc parler d'une progression constante en matière de sécurité des données. Cela ne revient pas à dire qu'il ne faut faire confiance à personne, car cela supposerait alors de retourner à une page non numérique. Je pense en tout cas que l'on peut réfuter l'idée qu'il y a un droit au mensonge dans la vie privée, car tout se découvre très vite – c'est aussi vrai pour les mensonges d'Etat que d'entreprise – en revanche la lutte est constante, avec, pour chaque faille qui apparaît, un renforcement.

Aux Etats-Unis, les déclarations d'une entreprise auprès de ses utilisateurs, si elles ne sont pas respectées, même au corps défendant de l'entreprise, sont beaucoup plus lourdement sanctionnées qu'elles ne le sont dans l'Union européenne. C'est cela qui amène la sanction de Snapchat par la FTC. En Europe nous savons que la sécurité est relative, ce qui, culturellement, nous pousse moins à imputer un mensonge par omission ou négligence comme cela se fait aux Etats-Unis. Sur le terrain de la sécurité, il est faux de croire que la vie privée est plus protégée en Europe qu'aux Etats-Unis. Ces derniers ont adopté ces règles de notification publique de faille de sécurité à partir de 2003, alors que cela ne date que de 2009 en Europe, et ne vaut que pour les acteurs des télécoms.