Faille de sécurité Facebook : recours contre la fuite des données personnelles

publié le **13/05/2011**, vu **4198 fois**, Auteur : Anthony BEM

Facebook annonce avoir corrigé une importante faille de sécurité. Bien que jusqu'à présent il n'existe aucune preuve démontrant une quelconque utilisation malveillante des données personnelles des 600 millions de membre, Facebook prends de gros risques juridiques au travers de cette négligence.

Symantec, l'éditeur de logiciels antivirus qui est à l'origine de la découverte cette faille, a prévenu les responsables de Facebook qui a aussitôt pris les mesures nécessaires.

Tout d'abord, un peu de technique.

Les développeurs d'application sur Facebook utilisent un SSO (« *Single Sign-On* » ou une « *authentification unique* ») qui concrètement permet à un utilisateur de ne se servir que d'un seul protocole d'authentification pour accéder à une pluralité de services.

S'agissant de Facebook, l'utilisateur peut accéder aux services fournis par les applications en donnant simplement son autorisation. L'identifiant et le mot de passe ne sont exigés qu'une seule fois ou ne sont pas exigés du tout.

L'avantage pour les entreprises qui utilisent cette procédure réside dans la simplicité et la rapidité de mise en œuvre d'une procédure d'inscription.

On évite ainsi ce que certains appellent la « *fatigue du mot de passe* ».

Par exemple, lorsqu'un utilisateur se connecte à *Deezer, MusicMe, Netvibes* et les derniers forums de discussions ou tout autre site internet utilisant l'authentification par le biais d'un profil Facebook existant, il permet au programme utiliser par l'un des sites internet précités de créer un « *token* », l'équivalent numérique d'une clef de rechange, qui évite à l'utilisateur d'avoir à s'authentifier en permanence sur ces sites.

La faille de Facebook concernait ce « *token* » qui était visible par les tiers et en particulier par les régies publicitaires.

Or, c'est à partir du « *token* » que l'application peut accéder aux informations de l'utilisateur.

Plus juridiquement, le SSO a deux incidences :

- il implique des obligations respectives entre les parties (I) ;
- le transfert des données que le droit qualifie de «personnelles» et qui est réglementé (II).

I - Une relation contractuelle tripartite

Juridiquement, le SSO est une relation tripartite entre :

- L'utilisateur
- Le prestataire d'authentification (Facebook, Google, etc.)
- Le développeur qui utilise le SSO pour authentifier ses utilisateurs

À chaque niveau, il existe une relation contractuelle :

- **Entre l'utilisateur et le prestataire d'authentification** : Il y a acceptation des Conditions générales d'utilisation du service, ainsi que tous les documents prévus par le prestataire tels que la politique de confidentialité, etc…. Cette acceptation, qui peut se découvrir du simple usage du service, fait entrer l'utilisateur dans une relation contractuelle dont il n'a, le plus souvent, pas conscience.

- **Entre le prestataire d'authentification et l'entreprise qui utilise le SSO** : L'intégration du SSO implique une acceptation de conditions générales de la part de l'entreprise qui souhaite utiliser cette méthode d'authentification.

- **Entre l'utilisateur et l'entreprise qui utilise le SSO** : L'utilisateur accepte le transfert de ses données de connexion vers l'entreprise utilisatrice.

En fonction du niveau de ces relations contractuelles, des termes par lesquels chacune de ces trois parties s'engage, la responsabilité contractuelle de l'un et/ou de l'autre peut, le cas échéant, être engagée.

Dans ce contexte, si le site internet Facebook ne respecte pas sa politique de confidentialité (comme c'est peut-être le cas dans cette dernière affaire de fuite de données), il est susceptible de voir sa responsabilité engagée.

II - La protection des données personnelles dans le cadre d'un SSO

2.1 – La problématique de la collecte indirecte des données personnelles

Le développeur d'une application se trouve dans une situation de **collecte indirecte des données de l'utilisateur**. En effet, il s'adresse au prestataire de SSO (Facebook, Google, etc.) pour obtenir les données nécessaires à une authentification.

Or la collecte indirecte comporte certaines particularités, explicitées par l'article 32-III de la Loi informatique et liberté modifiée sur ce point en 2004 :

> *Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.*

Les informations énumérées au I sont notamment :

> - L'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
>
> - La finalité poursuivie par le traitement auquel les données sont destinées ;
>
> - Les destinataires ou catégories de destinataires des données ;
>
> - Les droits qu'elle (la personne concernée) tient des dispositions de la section 2 du présent chapitre (c'est-à-dire le droit d'accès et de rectification aux données).

Cette contrainte peut être éludée de deux façons :

- Par une acceptation du SSO par l'utilisateur (par un pop up par exemple). C'est cette méthode qu'utilise Facebook.

- Par une information de l'utilisateur (par mail par exemple) de la collecte de ses données de connexion.

Le développeur a tout intérêt à utiliser les deux méthodes, s'assurant ainsi de la complète information de l'utilisateur du service.

Quoi qu'il en soit, Facebook est susceptible de mettre sa responsabilité en jeu s'il s'avère que la firme (en tant que responsable du traitement de données) n'a pas respecté les obligations légales précitées,

2.2 – Les recours contre la perte ou le vol de données personnelles

Plusieurs recours existent et permettent de réparer les conséquences de la perte ou du vol de données à caractère personnel et confidentiel.

2.2.1 – Le délit de manquement à la sécurisation des données

Selon l'article 226-17 du Code pénal :

> *« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.»*

L'article 34 de la loi informatique et libertés cité dans le corps de l'article 226-17 précise que :

> *« Le responsable du traitement est tenu de prendre toutes précautions utiles , au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »*

Le délit de défaut de « *précautions utiles* » précité nécessite de faire la démonstration d'un élément matériel et d'un élément moral du délit.

La matérialité de l’infraction apparait suite à la preuve du manquement.

En d’autres termes, il convient d’établir que, techniquement, les moyens mis en œuvre pour la protection des données (cryptologie, contrôle, vérification, etc...) étaient insuffisants, par le biais d’une expertise ou éventuellement grâce au travail de la CNIL.

Concernant l’aspect moral de l’infraction, la simple imprudence suffit à le caractériser.

2.2.2 - Le délit de divulgation illicite de certaines données personnelles

L’article 226-22 du Code pénal incrimine :

> *« Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ».*

La divulgation prévue à l'alinéa précédent est punie de cinq ans d'emprisonnement et de 300.000 euros d'amende ou de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Ainsi, la simple imprudence suffit à faire état de l’élément moral de l’infraction.

Toutefois, la matérialité des faits est plus délicate à apporter.

Il faut dans un premier temps démontrer que cette divulgation a porté atteinte à la vie privée.

Il faut ensuite que la divulgation ait eu lieu sans l’autorisation de la personne concernée.

Il faut enfin que le destinataire des informations ne soit pas habilité à les recevoir. Sur ces points, il peut y avoir débat.

2.2.3 – Violation du secret professionnel

En outre, l’article 226-13 Code pénal réprime :

> *« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende »*

Ce texte s’applique en apparence à certains corps de métier. Ainsi le médecin, le banquier ou même l’avocat, sont soumis à ce secret.

Cependant rien n’interdit de penser que le secret professionnel puisse s'appliquer, non seulement aux professions soumises à cette obligation, mais également à tout autre professionnel qui détient des secrets qui lui sont confiés par des particuliers.

Il sera donc intéressant de suivre l’évolution de ces nouvelles applications et leur traitement juridique en cas de préjudices.

Je suis à votre disposition pour toute information ou action.

PS : Pour une recherche facile et rapide des articles rédigés sur ces thèmes, vous pouvez taper vos "mots clés" dans la barre de recherche du blog en haut à droite, au dessus de la photographie.

Anthony Bem
Avocat à la Cour
27 bd Malesherbes - 75008 Paris
Tel : 01 40 26 25 01

Email : abem@cabinetbem.com

www.cabinetbem.com