FaceApp : 2 choses à savoir pour sauver ses données

La frénésie autour de l'application FaceApp a rapidement tourné à des appels à la vigilance sur l'utilisation des données privées à l'insu des utilisateurs. Mais aussi sur les premières escroqueries qii exploite le phénomène.

1- La Cnil met en garde sur les conditions d'utilisation des données

La première l'a fait sous la forme de conseils relatifs aux applications de retouche photo.
Une catégorie dont FaceApp relève avec ses filtres modificateurs de visages.

« *L'attractivité ou le caractère ludique du service proposé ne doit pas occulter les éventuelles contreparties concernant l'utilisation de vos données personnelles* », explique la Cnil.

> *#Faceapp et autres applications de retouche photo : les conseils de la @CNIL à l'attention des utilisateurs??* *https://t.co/2OyHmtYnUu pic.twitter.com/RgbQEKnDSn*
>
> — *CNIL (@CNIL) 19 juillet 2019*

Et de rappeler que l'entreprise doit préciser à l'utilisateur si ses photos sont :

- stockées ou non dans l'UE (et combien de temps elle sont conservées) ;
- communiquées à des tiers ;
- réutilisées à d'autres fins, typiquement publicitaires ;
- et s'il existe, pour l'utilisateur, un moyen d'exercer ses droits RGPD

Attention également, toujours selon la Cnil, aux applications qui fonctionnent en tâche de fond et continuent à collecter des données.

On gardera aussi à l'esprit que les photos qu'on partage peuvent inclure des métadonnées comme la géolocalisation.

Ces conseils sont d'autant plus importants avec FaceApp que les développeurs de l'application se sont réservé de nombreux droits en matière d'exploitation des contenus.

2 – FaceApp Pro : une appli qui n'existe pas

Du côté d'ESET, éditeur de logiciels de sécurité, on s'est fait l'écho d'une fausse version « pro » de FaceApp.

Celle-ci est exploitée de deux manières :

- Un faux site web sur lequel on est censé pouvoir la télécharger. Sauf que pour aller au bout du processus, il faut visionner des publicités, répondre à des enquêtes, installer d'autres applications ou encore accepter les notifications en provenance de certains sites.
  La version téléchargée est la même que celle qu'on trouve sur Google Play.
- Des vidéos YouTube qui promeuvent des liens de téléchargement de ce même FaceApp Pro.
  Les liens déclenchent en fait le téléchargement d'autres applications… potentiellement malveillantes.

Photo d'illustration © FaceApp Inc