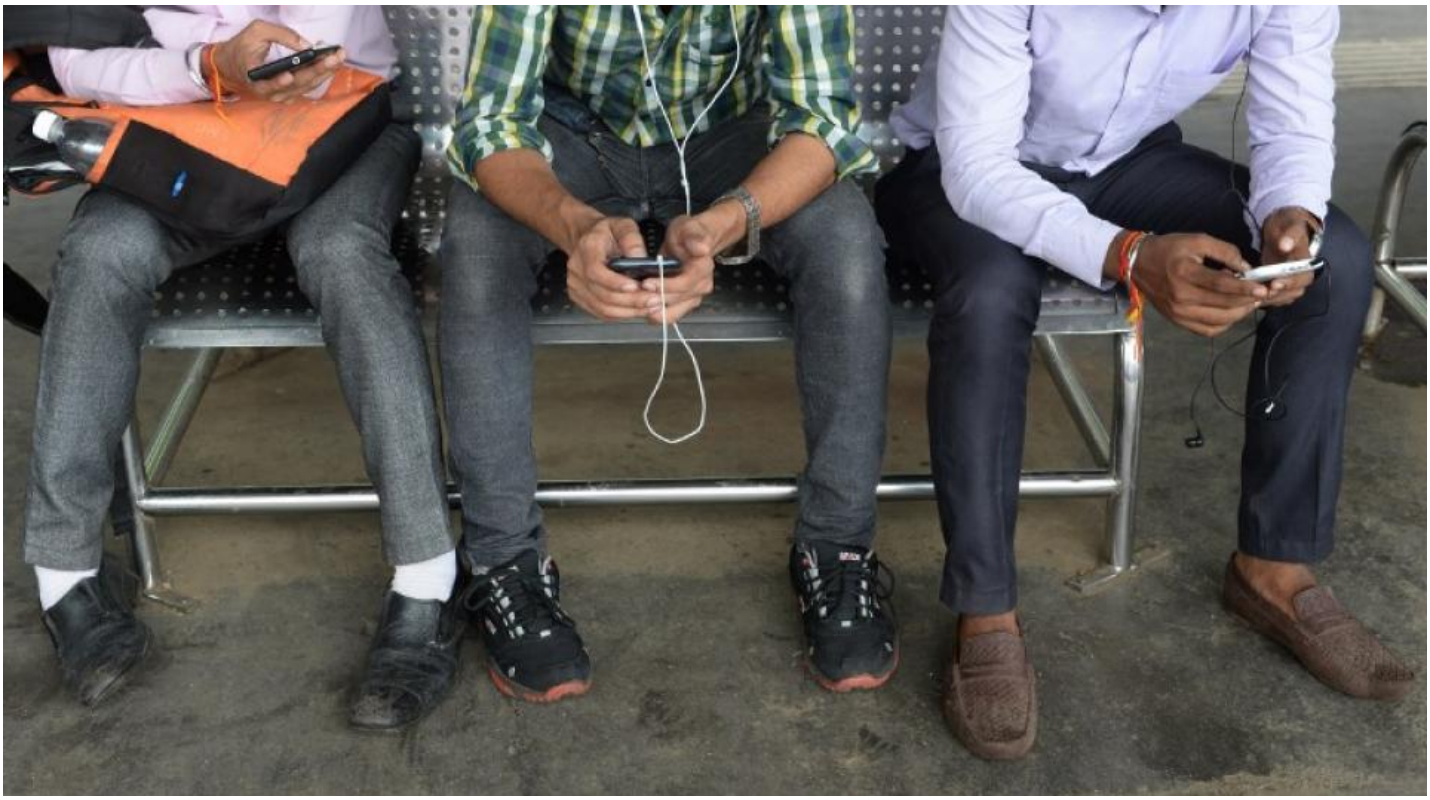
18 juillet 2019

Données personnelles

Dans la jungle des conditions générales d'utilisation : savez-vous vraiment à quoi vous consentez lorsque vous utilisez des applications de reconnaissance faciale ?



L'énorme succès de l'application FaceApp interroge sur un problème plus complexe. La récupération de données personnelles est un enjeu économique majeur pour ce type d'entreprises et peu d'utilisateurs prennent le temps de s'informer sur l'utilisation de ces données.

Avec Claude-Etienne Armingaud

Atlantico : Certaines applications qui permettent à une personne de modifier des photos prises sur son portable avec des filtres divertissants disposent de conditions générales d'utilisation particulièrement gênantes. L'une d'entre elles, FaceApp, demande par exemple l'autorisation d'utiliser l'image de l'utilisateur à n'importe quel moment. Faut-il mettre ce problème sur le dos du consommateur imprudent, ou sur celui des services numériques qui rédigent volontairement des clauses de ce type ? Les conditions générales ne sont-elles pas généralement trop complexes, trop nombreuses ou trop longues pour que l'accord de l'utilisateur ait une validité juridique ?

Claude-Etienne Armingaud : On voit ici l'un des effets pervers de la viralité des usages au travers de l'environnement numérique et, dans une certaine mesure, ce que les anglo-saxons appellent le FoMo (« Fear of Missing out ») -- tout le monde le fait, et je veux en être.

Si en France, les contrats légalement formés tiennent lieu de loi à ceux qui les ont faits (Article 1103 du Code Civil français), cette absolutisme contractuel est encore plus vrai outre-Atlantique. La peur du manque décrite ci-dessus conduit souvent à installer des applications et utiliser des services rapidement, sans lire des conditions générales qui, ne l'oublions pas, constituent un contrat entre l'éditeur du services et l'utilisateur, et qu'un contrat engage.

A cet égard, les éditeurs de services ont besoin de certains droits de la part des utilisateurs pour pouvoir fournir leur service -- c'est le cas, par exemple, d'une licence sur le contenu pour que l'éditeur puisse héberger, copier, et effectuer d'autres diligences au nom et pour le compte de l'utilisateur, sans risquer de se voir attaquer pour contrefaçon de droits d'auteur sur les images.

Cependant, la tentation est parfois grande de s'octroyer des droits le plus largement possible, notamment aux fins de monétiser, directement (en vendant ces images à des tiers) ou indirectement (en utilisant ces images pour la publicité des services). Cette utilisation n'est pas strictement nécessaire à la fourniture des services mais peut l'être pour qu'une telle fourniture de services soit gratuite pour l'utilisateur.

En parallèle, la nouvelle réglementation européenne (Règlement Général sur la Protection des Données, le fameux RGPD) impose une transparence totale des fournisseurs de services sur les traitements mis en œuvre. Il faut donc se féliciter que cette clause soit

présente par souci de transparence, plutôt que cette fonction soit effectivement utilisée à l'insu des personnes.

Néanmoins, et surtout depuis l'entrée en vigueur en 2018 du RGPD, l'inflation textuelle est énorme. En 2012, déjà, les recherches de l'université de Carnegie Mellon à Pittsburgh établissait que la lecture complète des conditions d'utilisation et politique de confidentialité validées par an et par utilisateur représenterait en moyenne 76 journées de travail ! (source : The Cost of Reading Privacy Policies, A Journal of Law and Policy For the Information Society) .

Il serait dès lors illusoire de penser que tout le monde lit tout, peu important les obligations de transparence requises par le droit.

Heureusement, l'Europe se distingue des États-Unis par sa forte protection des consommateurs - il faut non seulement que l'information soit disponible, mais également qu'elle soit en conformité avec ces obligations protectrices, au risque de se voir déclarée inapplicable !

Cette bataille a déjà commencé -- l'UFC Que Choisir a d'ores et déjà remporté un combat similaire contre Twitter en 2018 (TGI Paris, 7 août 2018) et Google en 2019 (TGI Paris, 12 février 2019). Si ces décisions ont fait l'objet de plusieurs années de procédures, et que des appels sont susceptibles de renverser le schéma, la tendance est à l'activisme européen pour protéger les utilisateurs, parfois vis-à-vis d'eux-mêmes, et de forcer les éditeurs à simplifier leur démarche envers leurs utilisateurs.

Dans le cas de FaceApp, les conditions d'utilisation et la politique de confidentialité pré-datent l'entrée en vigueur du RGPD (2017) et l'éditeur, qui semble être une société russe (et donc en dehors de l'Union Européenne), ne respecte pas les nouveaux critères d'applicabilité de la réglementation européenne…

Comment ce genre de problèmes est-il pris en compte par nos législations, par exemple le RGPD ?

En effet, le RGPD a vocation à s'appliquer *non solum* à toute entreprise mettant en œuvre des traitements dans le cadre d'un établissement stable dans l'Union européenne, *sed etiam* aux entités étrangères, si elles dirigent leurs services vers des utilisateurs européens. Si les lignes directrice du Comité Européen pour la Protection des Données sur la territorialité n'ont pas encore fait l'objet d'une révision après la consultation opérée en fin d'année 2018, leurs versions actuelles établissent des critères d'évaluation qui nous semblent pérennes : si une service, fourni par une société non européenne et non francophone, est disponible sur un magasin d'application européen, dans une langue européenne autre que celle du lieu d'établissement (par exemple, le français pour des américains ou des russes), et est tarifé en euros, l'offre de service à direction d'un public européen est difficilement contestable.

Dès lors, le RGPD vient protéger, en plus du droit de la consommation, les utilisateurs. Le grand message envoyé par ce Règlement est que les données à caractère ne sont pas une simple marchandise qui peut librement s'échanger sur une place de marché, mais qu'elles sont intrinsèquement liées à la personne dont elles émanent et constituent une composante de sa personnalité et un droit fondamental. En conséquence, une action, individuelle ou collective, pourrait être envisagée à l'encontre des sociétés peu scrupuleuses, tentées d'utiliser de manière trop large les données des utilisateurs, au-delà de ce qu'il serait strictement nécessaire pour les finalités légitimes envisagées, en application du principe de minimisation posé par le RGPD… et depuis les affaires menées tambour battant par la CNIL en France et l'ICO au Royaume Uni, les sanctions peuvent dissuasives, surtout pour des jeunes sociétés innovantes.

Dans l'attente d'une rationalisation des acteurs, le pouvoir reste *in fine* dans les mains des utilisateurs. Et s'il avère que les conditions d'utilisation sont trop exigeantes, il demeure toujours possible de faire directement valoir ses droits à l'encontre de la société en question -- à commencer à désinstaller l'application et d'exiger la mise en œuvre des droits d'accès et d'effacement des données ainsi que d'opposition au traitement !