



Lancé sur Facebook, le 10 years Challenge connaît un immense succès sur les réseaux sociaux. Le défi consiste à publier deux photos prises à dix ans d'écart. Damon Lane, un météorologue américain, aurait été le premier internaute à participer au challenge, le 11 janvier 2019.

Depuis quelques jours, plusieurs internautes ont commencé à publier leurs participations au challenge. Seulement, pas tous les internautes ne s'y lancent les yeux fermés.

C'est le cas de **Kate O'Neill**, fondatrice de KO Insights et auteur de Tech Humanists.

Dans un article pour le magazine Wired, O'Neill alerte sur les dérives sécuritaires qui peuvent se cacher derrière ce nouveau challenge, en apparence inoffensif. Elle se demande jusqu'où pourrait aller l'exploitation de ces photos « before/after ».

Elle pointe 3 cas d'utilisation de ces données: un honorable, un mercantile et un risqué.

Dans le premier cas, la technologie de la reconnaissance faciale aiderait à retrouver des enfants disparus. En Inde, par exemple, 3000 enfants disparus ont été retracés, en seulement 4 jours, grâce à cette technologie.

Dans le second cas, l'objectif est de se faire de l'argent grâce aux informations personnelles des utilisateurs Facebook. Les publicitaires pourraient profiter de l'occasion pour mieux cibler leurs campagnes marketing.

Dans le troisième cas, les dérives sont plus lourdes. Ce challenge pourrait servir, par exemple, de nouvel indice de santé aux compagnies d'assurance. Si vous vieillissez visiblement plus vite que vos semblables, vous pourriez payer plus cher votre assurance-vie.

Un risque pour votre vie privée ?

O'Neill donne l'exemple d'Amazon. En 2016, l'entreprise a introduit un service de reconnaissance faciale en temps réel. Ensuite, le géant de l'e-commerce a vendu ces données à la police. Bonne nouvelle pour les services de police qui pouvaient utiliser ses données pour tracker les personnes suspectées de crime. Mais il pourrait également servir pour reconnaître n'importe quelle personne qui dérange comme des militants ou activistes.

Les participants au challenge donnent directement accès à des éléments de leur vie privée, en les contextualisant. Leur parcours de vie et leur changement physique sont tracés et peuvent être exploités de diverses manières.

“Ce challenge permet une identification formelle et permet de reconnaître la personne dans des contextes et à des époques différentes”,

explique **Olivier Bogaert**, Commissaire à la Computer Crime Unit.



Lesmoutonsrebelles.com