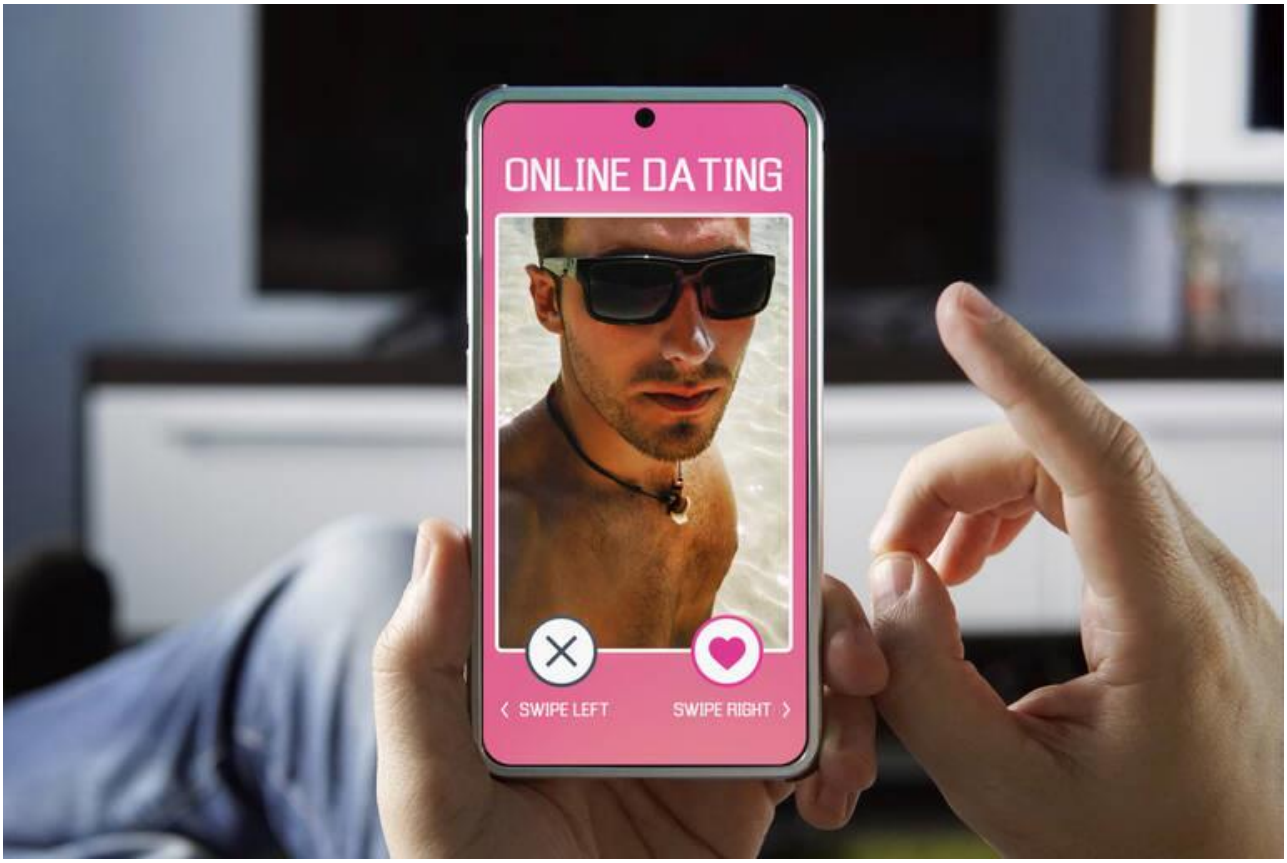
Les 400 culs

Les sites de rencontres dans la chasse aux faux profils

Article réservé aux abonnés

Reconnaissance faciale, carte d'identité, système de notation… En réponse à la multiplication de faux comptes, les applications de rencontres n'hésitent plus à faire passer des contrôles et certifier leurs utilisateurs. Suffisant ?



L'appli Joyce est une des premières à faire passer ses membres par l'équivalent d'un contrôle de sécurité. (Diy13/Getty Images/iStockphoto)

par Agnès Giard
publié aujourd'hui à 10h31

En mars, dans le petit village de Beussent, dans le nord de la France, un homme est mis en examen pour le meurtre de sa compagne, Alicia, 28 ans. Il l'a tuée alors qu'il entretenait une relation avec Béatrice, une femme qui n'existe pas, «rencontrée» sur Facebook. Le profil de Béatrice est en réalité celui d'un «brouteur» – un escroc spécialisé dans la simulation de sentiments –, originaire de Côte-d'Ivoire. Ce féminicide aurait-il pu être évité ? Pour en finir avec les faux comptes créés par des arnaqueurs, la plupart des applications de rencontre cherchent à rendre leurs plateformes plus sûres. Pour s'assurer que les utilisateurs ne mentent pas sur leur identité, certaines emploient les grands moyens. C'est le cas de Joyce, une des premières (sinon la toute première) à faire passer ses membres par l'équivalent d'un contrôle de sécurité.

Billet
Données personnelles exploitées, prolifération des discriminations… Il est temps de désinstaller Grindr
High tech
23 avr. 2024

Lancée en 2017, cette application de rencontres allemande propose un système de «vérification» qu'il est tout à fait possible de refuser, mais… les membres sont priés d'envoyer une vidéo montrant leur visage et leur carte d'identité en gros plan. Chaque profil «authentifié» obtient son coup de tampon. Au passage, le profil est corrigé. Si vous avez menti sur votre âge, par exemple, ou sur la couleur de vos yeux, un modérateur rend les données conformes à la vérité puis vous envoie un message : *«Félicitations, ta vidéo a été validée. Une coche blanche se trouve désormais derrière ton nom de profil. Afin d'obtenir la coche verte, il faut qu'au moins cinq autres membres vérifiés te signalent dans leurs contacts comme une personne qu'ils connaissent personnellement.»* Il n'y a alors plus qu'à matcher des partenaires. La vidéo, quant à elle, est immédiatement détruite, afin de protéger la vie privée des personnes inscrites. En théorie, aucun danger.

Certificat d'humain «authentique»

«Environ 60 % des membres font valider leur identité dans les quarante-huit heures qui suivent leur inscription, affirme Louiza Papadopoulou, directrice marketing international de la compagnie Joyclub qui a développé l'app. *En France, nous offrons une adhésion premium aux personnes authentifiées en guise de récompense. Il s'agit de motiver les inscrits pour qu'ils contribuent à créer un environnement protégé pour toute la communauté.»* Ainsi qu'elle le souligne, la demande est forte : depuis quelques années, beaucoup d'utilisateurs, hommes et femmes, se plaignent d'abus. La logique concurrentielle des applis de rencontre pousse en effet de nombreuses personnes à modifier leur apparence. Photos retouchées, corps embellis : la rencontre dans la vraie vie réserve parfois de mauvaises surprises. La multiplication des faux comptes entretient également la suspicion en ligne. Quel arnaqueur potentiel se cache derrière une jolie inconnue ? Dès 1993, le magazine *The New Yorker* publiait cet avertissement sous la forme d'un dessin humoristique : *«Sur internet, personne ne sait que vous êtes un chien.»*

A lire aussi
Anonymat, VPN, bannissements… Le projet de loi sur Internet fait polémique
Politique
19 sept. 2023

Trente ans plus tard, fin 2023, les parlementaires français discutent du projet de loi sur la «sécurité numérique», examinant la possibilité que les réseaux sociaux puissent proposer aux utilisateurs de déposer des preuves d'identité. *«Les actes frauduleux de certains utilisateurs font souvent les gros titres»,* confirme Rémi Slama, avocat international spécialisé en droit des nouvelles technologies (vie privée, cybersécurité et intelligence artificielle), exerçant au sein du cabinet Fasken, qui mentionne notamment le *«chantage aux photos dénudées»,* orchestré par des réseaux opérant en Afrique ou en Europe de l'Est.

«Le rôle de la communauté est crucial»

Pour rassurer leurs utilisateurs, beaucoup d'applis offrent maintenant des outils certifiant que le profil d'une personne en ligne correspond bien à la réalité. Un quart de ses utilisateurs étant victimes d'arnaques (selon les chiffres 2023 de l'entreprise Norton), Tinder se démène pour traquer les faussaires. Cela commence, vers 2021, avec un système de reconnaissance faciale. Les inscrits doivent envoyer des selfies qui sont comparés avec les photos publiées sur leur compte. Gare aux imposteurs !

Depuis 2023, le système d'analyse biométrique est renforcé : il s'agit d'envoyer un selfie vidéo, plus difficile à falsifier qu'une simple photo. Pour compliquer la tâche des fraudeurs, l'application demande à l'utilisateur de prendre une pose parmi environ cent poses différentes, envoyées de façon aléatoire : clin d'œil, bouche en «O», sourcils dressés… Mais est-ce suffisant ? Apparemment pas. Pour sécuriser leurs échanges, certains utilisateurs n'hésitent pas à télécharger des outils comme TrustedDate, par exemple, *«1er organisme de certification des profils numériques sur les sites de rencontres»*. Tout comme l'appli Joyce, pionnière du système, TrustedDate demande aux utilisateurs une copie de leurs papiers d'identité.

«Les processus d'authentification par document d'identité ou par selfie se généralisent mais sont souvent facultatifs», note Rémi Slama, en soulignant la difficulté : dans le domaine de la rencontre en ligne, qui présuppose souvent l'échange d'informations intimes (orientation sexuelle, fantasmes ou pratiques bizarres)

on ne peut pas imposer aux gens qu'ils s'identifient. *«Dans le contexte de l'Union européenne, notamment, il serait nécessaire d'obtenir le consentement éclairé des utilisateurs avant de leur demander de présenter leur carte d'identité en ligne ou de se filmer,* explique l'avocat. *De plus, la demande de carte d'identité présentée en ligne devrait être justifiée par une raison légitime et nécessaire. Cela impliquerait des mesures telles que le cryptage des données, la sécurisation des serveurs, la limitation de l'utilisation des données à des fins spécifiques, et l'adoption de politiques de confidentialité transparentes…»* Bien que les créateurs d'applis ou de sites de rencontres affirment tous offrir des plateformes protégées contre le piratage, comment savoir si l'on est vraiment à l'abri ?

A lire aussi
Tinder détox : «Depuis que j'ai arrêté les applis, j'ai fait de belles rencontres dans des contextes inattendus»
Intimités
22 mars 2024

Une violation de données est si vite arrivée… Il devient par ailleurs si facile de tricher grâce aux *deep fakes*… Comment vérifier qu'une photo, une voix ou une vidéo, ne sont pas générées par intelligence artificielle ? Pour la plupart des utilisateurs, la solution idéale reste peut-être la cooptation. *«Un système de vérification technique ne peut suffire seul,* confirme Louiza Papadopoulou. *Le rôle de la communauté est crucial. Il faut que les membres soient proactifs et signalent les profils qui semblent suspects.»* Ainsi qu'elle le défend, seul un *«effort de collaboration»* peut permettre aux utilisateurs de se protéger contre les faux profils. A chacun d'être *«vigilant»,* suggère-t-elle. De fait, un nombre croissant d'apps proposent maintenant le système de notation en cas de mauvais comportement. Ce système, censé éliminer les usurpateurs mais aussi les tricheuses, les menteurs ou les personnes non fiables, présente cependant lui aussi ses défauts. Que faire si une personne en «dénonce» une autre par vengeance ? N'est-il pas dangereux d'encourager les gens à s'évaluer les uns les autres alors qu'ils sont censés livrer leur cœur ou leur corps en confiance ?