



Torino, Settembre 2021



## Deepfake, il falso che ti “ruba” la faccia e la privacy



• Consulting • Excellence • Outsourcing

**RECONSULT S.r.l.**  
Via Legnano, 31  
10128 Torino  
[www.reconsultsrl.it](http://www.reconsultsrl.it)

Telefono 011. 381. 68. 00  
Telefono 011. 381. 67. 33  
Fax 011. 381. 67. 27  
email [welcome@reconsultsrl.it](mailto:welcome@reconsultsrl.it)

Capitale Sociale Euro 30.000,00 i.v.  
R.E.A., C.C.I.A.A. To n° 1024131  
Reg. Soc. To, Codice fiscale e  
Partita IVA 09096000014



## Cos'è un deepfake



I deepfake sono foto, video e audio creati grazie a software di intelligenza artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

La parola deepfake è un neologismo nato dalla fusione dei termini “fake” (falso) e “deep learning”, una particolare tecnologia AI. Le tecniche usate dai deepfake sono simili a quelle delle varie app con cui ci si può divertire a modificare la morfologia del volto, a invecchiarlo, a fargli cambiare sesso, ecc. La materia di partenza sono sempre i veri volti, i veri corpi e le vere voci delle persone, trasformati però in “falsi” digitali.

Negli ultimi tempi hanno iniziato a diffondersi app e software che rendono possibile realizzare deepfake, anche molto ben elaborati e sofisticati, utilizzando un comune smartphone.

La diffusione dei deepfake è di conseguenza notevolmente aumentata, e con essa i rischi connessi.



• Consulting • Excellence • Outsourcing

**RECONSULT S.r.l.**  
Via Legnano, 31  
10128 Torino  
[www.reconsultsrl.it](http://www.reconsultsrl.it)

Telefono 011. 381. 68. 00  
Telefono 011. 381. 67. 33  
Fax 011. 381. 67. 27  
email [welcome@reconsultsrl.it](mailto:welcome@reconsultsrl.it)

Capitale Sociale Euro 30.000,00 i.v.  
R.E.A., C.C.I.A.A. To n° 1024131  
Reg. Soc. To, Codice fiscale e  
Partita IVA 09096000014



## Il deepfake e il furto di identità



Quella realizzata con i deepfake è una forma particolarmente grave di furto di identità.

Le persone che compaiono in un deepfake a loro insaputa non solo subiscono una perdita di controllo sulla loro immagine, ma sono private anche del controllo sulle loro idee e sui loro pensieri, che possono essere travisati in base ai discorsi e ai comportamenti falsi che esprimono nei video.

Le persone presenti nei deepfake potrebbero inoltre essere rappresentate in luoghi o contesti o con persone che non hanno mai frequentato o che non frequenterebbero mai, oppure in situazioni che potrebbero apparire compromettenti.

In sostanza, quindi, un deepfake può ricostruire contesti e situazioni mai effettivamente avvenuti e, se ciò non è voluto dai diretti interessati, può rappresentare una grave minaccia per la riservatezza e la dignità delle persone.



• Consulting • Excellence • Outsourcing

**RECONSULT S.r.l.**  
Via Legnano, 31  
10128 Torino  
[www.reconsultsrl.it](http://www.reconsultsrl.it)

Telefono 011. 381. 68. 00  
Telefono 011. 381. 67. 33  
Fax 011. 381. 67. 27  
email [welcome@reconsultsrl.it](mailto:welcome@reconsultsrl.it)

Capitale Sociale Euro 30.000,00 i.v.  
R.E.A., C.C.I.A.A. To n° 1024131  
Reg. Soc. To, Codice fiscale e  
Partita IVA 09096000014



## Deepfake e cyberbullismo



I video deepfake possono essere creati ad hoc per realizzare veri e propri atti di cyberbullismo, che hanno come vittime soprattutto giovani.

Un deepfake può essere realizzato per denigrare, irridere e screditare le persone coinvolte, o addirittura per ricattarle, chiedendo soldi o altro in cambio della mancata diffusione del video oppure per la sua cancellazione se è già stato diffuso.



• Consulting • Excellence • Outsourcing

**RECONSULT S.r.l.**  
Via Legnano, 31  
10128 Torino  
[www.reconsultsrl.it](http://www.reconsultsrl.it)

Telefono 011. 381. 68. 00  
Telefono 011. 381. 67. 33  
Fax 011. 381. 67. 27  
email [welcome@reconsultsrl.it](mailto:welcome@reconsultsrl.it)

Capitale Sociale Euro 30.000,00 i.v.  
R.E.A., C.C.I.A.A. To n° 1024131  
Reg. Soc. To, Codice fiscale e  
Partita IVA 09096000014



## Deepfake e fake news



I deepfake possono riguardare politici o opinion leader, con lo scopo di influenzare l'opinione pubblica. Video deepfake possono ad esempio essere mostrati o inviati agli elettori che simpatizzano per un determinato personaggio politico, rappresentandolo mentre compie azioni poco lecite o mentre si trova in situazioni sconvenienti, allo scopo di screditarlo ed influenzare le opinioni o il voto. In questo modo, i deepfake possono purtroppo contribuire alla diffusione di fakenews e alla disinformazione.

Il deepfake può quindi arrivare a privare le persone della cosiddetta "autodeterminazione informativa" ("ciò che voglio far sapere di me lo decido io"), come pure ad incidere sulla loro libertà decisionale ("quello che penso e faccio è una scelta su cui gli altri non possono interferire").



• Consulting • Excellence • Outsourcing

**RECONSULT S.r.l.**  
Via Legnano, 31  
10128 Torino  
[www.reconsultsrl.it](http://www.reconsultsrl.it)

Telefono 011. 381. 68. 00  
Telefono 011. 381. 67. 33  
Fax 011. 381. 67. 27  
email [welcome@reconsultsrl.it](mailto:welcome@reconsultsrl.it)

Capitale Sociale Euro 30.000,00 i.v.  
R.E.A., C.C.I.A.A. To n° 1024131  
Reg. Soc. To, Codice fiscale e  
Partita IVA 09096000014



## Deepfake e cybercrime



Il deepfake può essere utilizzato per attività telematiche illecite, come lo spoofing (il furto di informazioni che avviene attraverso la falsificazione di identità di persone o dispositivo, in modo da ingannare altre persone o dispositivi e ottenere la trasmissione di dati), il phishing e il ransomware.

Volti e voci artefatti possono essere utilizzati per ingannare i sistemi di sicurezza basati su dati biometrici vocali e facciali. Ad esempio, video o audio-messaggi deepfake creati da malintenzionati possono essere inviati ai nostri colleghi, amici o parenti per invitarli a cliccare su link o aprire allegati a messaggi che espongono pc, smartphone o altri dispositivi e sistemi a pericolose intrusioni, oppure per convincerli a fornire, ingannando la loro fiducia, informazioni e dati sensibili.

Inoltre oggi molti sistemi digitali (domotica, assistenti vocali, smartphone, nonché alcuni sistemi bancari o sanitari) ricorrono a dati biometrici vocali e facciali come sistema di autenticazione per l'accesso. Video e audio-messaggi deepfake potrebbero essere utilizzati per ingannare tali sistemi.



• Consulting • Excellence • Outsourcing

**RECONSULT S.r.l.**  
Via Legnano, 31  
10128 Torino  
[www.reconsultsrl.it](http://www.reconsultsrl.it)

Telefono 011. 381. 68. 00  
Telefono 011. 381. 67. 33  
Fax 011. 381. 67. 27  
email [welcome@reconsultsrl.it](mailto:welcome@reconsultsrl.it)

Capitale Sociale Euro 30.000,00 i.v.  
R.E.A., C.C.I.A.A. To n° 1024131  
Reg. Soc. To, Codice fiscale e  
Partita IVA 09096000014



## Come proteggersi dai deepfake

Le grandi imprese del digitale (piattaforme social media, motori di ricerca, ecc.) stanno già studiando e applicando delle metodologie per il contrasto al fenomeno, come algoritmi di intelligenza artificiale capaci di individuare i deepfake o sistemi per le segnalazioni da parte degli utenti, e stanno formando team specializzati nel monitoraggio e contrasto al deepfake. E le Autorità di protezione dei dati personali possono intervenire per prevenire e sanzionare le violazioni della normativa in materia di protezione dati.

Tuttavia, il primo e più efficace strumento di difesa è rappresentato sempre dalla responsabilità e dall'attenzione degli utenti.

### Ecco allora alcuni suggerimenti:

- Evitare di diffondere in modo incontrollato immagini personali o dei propri cari. In particolare, se si postano immagini sui social media, è bene ricordare che le stesse potrebbero rimanere online per sempre o che, anche nel caso in cui si decida poi di cancellarle, qualcuno potrebbe già essersene appropriato.
- Anche se non è semplice, si può imparare a riconoscere un deepfake. Ci sono elementi che aiutano: l'immagine può apparire pixellata (cioè un po' "sgranata" o sfocata); gli occhi delle persone possono muoversi a volte in modo innaturale; la bocca può apparire deformata o troppo grande mentre la persona dice alcune cose; la luce e le ombre sul viso possono apparire anormali.
- Se si ha il dubbio che un video o un audio siano un deepfake realizzato all'insaputa dell'interessato, occorre assolutamente evitare di condividerlo (per non moltiplicare il danno alle persone con la sua diffusione incontrollata). E si può magari decidere di segnalarlo come possibile falso alla piattaforma che lo ospita (ad esempio, un social media).
- Se si ritiene che il deepfake sia stato utilizzato in modo da compiere un reato o una violazione della privacy, ci si può rivolgere, a seconda dei casi, alle autorità di polizia (ad esempio, a la Polizia postale) o al Garante per la protezione dei dati personali.

Fonte: [Garante per la Protezione dei Dati Personali](#)



• Consulting • Excellence • Outsourcing