Deepfake low cost: con 50 dollari la tua voce può essere clonata

Maria Cattini | 03/10/2025 | Intelligenza Artificiale

Un tempo era un gioco da hacker esperti e ben finanziati. Oggi, bastano poche decine di dollari per creare un video o un audio deepfake credibile. La soglia economica è talmente bassa da rendere questa minaccia accessibile a chiunque: frodi, estorsioni e manipolazioni non richiedono più grandi investimenti ma soltanto una carta di credito e qualche minuto di registrazione vocale.

Sul web nascosto proliferano offerte “chiavi in mano”: pacchetti che promettono un video manipolato in poche ore, partendo da una foto o da una traccia audio di pochi secondi. Il risultato? Materiale pronto per campagne di truffa, ricatti o diffamazione.
Se ieri i deepfake erano legati a celebrità o politici, oggi chiunque può diventare bersaglio. La barriera economica si è sgretolata e questo apre scenari molto più concreti e pericolosi.

Le conseguenze vanno oltre la semplice curiosità tecnologica.

• Finanza: dirigenti “clonati” che ordinano bonifici milionari, sistemi vocali aggirati da voci false, aziende truffate con la complicità dell’IA.
• Reputazione: un video manipolato può distruggere carriere, relazioni e credibilità in poche ore.
• Diritto: se ogni filmato può essere falsificato, quanto valore avranno ancora le prove digitali in un’aula di tribunale? Difendersi sostenendo “è un deepfake” potrebbe diventare la norma.

Il vero nodo riguarda i dati biometrici. Voce e volto sono diventati il nuovo oro del cybercrime: non più password o numeri di carte di credito, ma ciò che rende unica la nostra identità.
Essere replicati digitalmente significa perdere il controllo su se stessi. Anche se il falso non viene diffuso, il solo fatto che esista può minare la fiducia attorno a una persona.

Contrastare i deepfake significa giocare una partita in cui i criminali hanno ancora un vantaggio.
Le prime soluzioni puntano su watermark digitali, algoritmi di rilevamento e sistemi di autenticazione avanzata. Ma la tecnologia da sola non basta.
Sul fronte normativo, l’Europa con l’AI Act ha iniziato a fissare obblighi di trasparenza per i sistemi generativi. Tocca però a imprese, professionisti della privacy e istituzioni collaborare per educare utenti e aziende a riconoscere e reagire ai falsi digitali.

Il fatto che clonare una voce costi meno di una cena fuori è un segnale: i deepfake non sono più un fenomeno marginale, ma un problema sociale e giuridico di massa.
Per chi lavora nella sicurezza, nella protezione dei dati o nel diritto digitale, la sfida è duplice: proteggere la dignità delle persone e difendere la fiducia collettiva nelle prove digitali.

Se il costo del falso scende, il valore della verità sale. Prepararsi oggi è l’unico modo per non pagarne domani il prezzo più alto.

□□ Vuoi capire come difenderti dai rischi dei deepfake? Seguici suTelegram e sulla nostra newsletter per ricevere guide pratiche e aggiornamenti.
Un tempo era un gioco da hacker esperti e ben finanziati. Oggi, bastano poche decine di dollari per creare un video o un audio deepfake credibile. La soglia economica è talmente bassa da rendere

questa minaccia accessibile a chiunque: frodi, estorsioni e manipolazioni non richiedono più grandi investimenti ma soltanto una carta di credito e qualche minuto di registrazione vocale.

Sul web nascosto proliferano offerte “chiavi in mano”: pacchetti che promettono un video manipolato in poche ore, partendo da una foto o da una traccia audio di pochi secondi. Il risultato? Materiale pronto per campagne di truffa, ricatti o diffamazione.
Se ieri i deepfake erano legati a celebrità o politici, oggi chiunque può diventare bersaglio. La barriera economica si è sgretolata e questo apre scenari molto più concreti e pericolosi.

Le conseguenze vanno oltre la semplice curiosità tecnologica.

• Finanza: dirigenti “clonati” che ordinano bonifici milionari, sistemi vocali aggirati da voci false, aziende truffate con la complicità dell’IA.
• Reputazione: un video manipolato può distruggere carriere, relazioni e credibilità in poche ore.
• Diritto: se ogni filmato può essere falsificato, quanto valore avranno ancora le prove digitali in un’aula di tribunale? Difendersi sostenendo “è un deepfake” potrebbe diventare la norma.

Il vero nodo riguarda i dati biometrici. Voce e volto sono diventati il nuovo oro del cybercrime: non più password o numeri di carte di credito, ma ciò che rende unica la nostra identità.
Essere replicati digitalmente significa perdere il controllo su se stessi. Anche se il falso non viene diffuso, il solo fatto che esista può minare la fiducia attorno a una persona.

Contrastare i deepfake significa giocare una partita in cui i criminali hanno ancora un vantaggio.
Le prime soluzioni puntano su watermark digitali, algoritmi di rilevamento e sistemi di autenticazione avanzata. Ma la tecnologia da sola non basta.
Sul fronte normativo, l’Europa con l’AI Act ha iniziato a fissare obblighi di trasparenza per i sistemi generativi. Tocca però a imprese, professionisti della privacy e istituzioni collaborare per educare utenti e aziende a riconoscere e reagire ai falsi digitali.

Il fatto che clonare una voce costi meno di una cena fuori è un segnale: i deepfake non sono più un fenomeno marginale, ma un problema sociale e giuridico di massa.
Per chi lavora nella sicurezza, nella protezione dei dati o nel diritto digitale, la sfida è duplice: proteggere la dignità delle persone e difendere la fiducia collettiva nelle prove digitali.

Se il costo del falso scende, il valore della verità sale. Prepararsi oggi è l’unico modo per non pagarne domani il prezzo più alto.

□□ Vuoi capire come difenderti dai rischi dei deepfake? Seguici su Telegram e sulla nostra newsletter per ricevere guide pratiche e aggiornamenti.