

I rischi che si corrono mettendo le foto dei figli sui social

Publicare immagini di minori sui social network è pericoloso per diversi motivi, tecnologici e psicologici

La sovraesposizione mediatica dei propri figli è certamente deleteria per diversi motivi tecnologici e psicologici. È quanto emerge dal rapporto Eurispes "Figli della rete: l'esposizione dei nostri figli online. **"È necessario pubblicare le foto dei propri figli?"**", si chiede l'Istituto di studi politici, economici e sociali. Un quesito che ricorre frequentemente la sociologia moderna di fronte all'esposizione incontrollata delle immagini di tantissimi minori sui social per mano dei genitori. Cosa ancora "più allarmante è che, pubblicando le foto dei figli minori, li si espone anche all'ingegneria sociale finalizzata all'adescamento da parte di persone malintenzionate. Pubblicare dettagli di vita privata sui social rappresenta un'arma in più per chi avvicina i pargoli con l'intento di guadagnare la loro fiducia attraverso una finta conoscenza dei parenti".

Per Eurispes, "la sovraesposizione mediatica dei propri figli è certamente deleteria per diversi motivi tecnologici. Il primo è sicuramente la probabile esposizione delle immagini del minore nei **circuiti pedofili, tramite fotomontaggi o addirittura video di tipo deep fake**". Altro fattore forse meno allarmante dal punto di vista psicologico, ma comunque esistente e di prospettiva futura, "è certamente quello di prevedere una probabilità che le immagini del proprio figlio finiscano, come avviene anche per le nostre, all'interno di piattaforme di riconoscimento facciale che utilizzano una mole impressionante di dati per poter **affinare i loro sistemi di intelligenza artificiale basati sul machine learning**".

Infine, conclude Eurispes, "c'è anche un ulteriore fenomeno che dovrebbe passare di moda ed è quello, come abbiamo visto dai top tweets, di utilizzare le immagini dei bambini per suscitare nel pubblico lo **stesso effetto dei famosi "gattini del web"**". "Fin quando si tratta di immagini riciclate dalla pubblicità, o da qualche stock di agenzia grafica, il discorso è certamente irrilevante come nel caso di TML, che guadagna likes e visibilità attraverso i Meme che trattano il connubio famiglia-figli-scuola. Se invece si lanciano iniziative che coinvolgono il pubblico in prima persona per guadagnare una premialità da parte dell' algoritmo del social network di riferimento, allora si sta inducendo gli utenti ad assumere atteggiamenti che vanno oltre il semplice intrattenimento".

Intorno ai figli c'è tutto un business di consulenze sia psicologiche che pedagogiche, didattica digitale e a distanza, rapporto genitore-figli e consigli per riuscire nell'impresa di padri e madri. Tuttavia **il genitore pubblica le foto o per vanità o per creare un archivio, questi incorre in due problematiche**: la prima è che si pubblicano le foto dei minori senza il loro consenso, la seconda è che un profilo social appartiene a una società che non ha un protocollo di tutela sui profili e può chiuderli e cancellarli definitivamente a suo piacimento. Questo ovviamente potrebbe essere un consiglio per limitare i danni derivanti dalla pubblicazione delle foto dei minori che appare, di giorno in giorno, un istinto quasi irrefrenabile.

Fonte: <https://www.pandasecurity.com/it/mediacenter/mobile-news/telegram-deepfake/>

Il bot di deepfake ha già fatto 100.000 vittime e le immagini manipolate vengono spesso utilizzate per fare revenge porn

I deepfake sono una delle ultime tendenze in materia di **manipolazione audio-video** e ne abbiamo già parlato ampiamente in relazione alla disinformazione. La situazione però si complica ulteriormente quando l'intelligenza artificiale consente di sviluppare **app di deepfake** come DeepNude, su cui si basa il **bot scoperto su Telegram**, che rendono i deepfake alla portata di tutti. Il bot semplifica a tal punto le cose, che è sufficiente inviare per chat una foto di una donna e questo restituirà la stessa immagine ma senza vestiti. Questo artificio è possibile grazie al **machine learning**: l'algoritmo analizza migliaia di immagini e impara a ricostruire l'aspetto del corpo femminile nudo in base alle informazioni che trova nella foto originale (dimensioni, ombre, proporzioni e così via). Ma l'aspetto davvero allarmante



è che questo bot funziona solo con le foto di donne, per cui sta diventando uno strumento di abuso e violenza di genere.

DeepNude, l'app di origine

Tutto parte dall'app **DeepNude**, sviluppata per divertimento e presto ritirata dal Web perché, a detta del suo creatore, "era diventata troppo pericolosa". Tuttavia, sappiamo che una volta pubblicato qualcosa su Internet, è praticamente impossibile cancellarne ogni traccia. Di fatto, il codice dell'app era già stato copiato e riprodotto prima del ritiro, ed è diventato disponibile su GitHub, il portale di casa Microsoft, insieme a varie modifiche e versioni successive. Ed ecco che qualcuno ha avuto un'altra idea brillante – si fa per dire – e ha creato un **bot per Telegram** su cui basta caricare le foto per ottenerne la versione senza vestiti. In modalità gratuita si riceve una foto con una filigrana, ovvero con dei segni in sovrainpressione. Pagando una cifra quasi simbolica si accede alla versione migliorata, ovvero senza filigrana, proprio come sui database online di fotografie come Shutterstock.

Così, alle polemiche sulla disponibilità del codice su GitHub si sono aggiunte quelle sulle norme e il controllo di Telegram. In realtà, anche qui non c'è niente di nuovo e il dilemma etico è ancora lontano dal trovare una soluzione: Internet dev'essere regolato? Se sì, fino a che punto? E chi lo decide, dato che non ci sono frontiere geografiche?

Indipendentemente dall'opinione di ognuno sull'**etica di Internet** (che in definitiva viene risolta in maniera sbrigativa da ciascuna corporation), rimane il problema di come le nuove tecnologie vengono utilizzate per umiliare o addirittura ricattare le donne. Questo è uno dei lati oscuri dei nuovi strumenti digitali, in particolare dell'intelligenza artificiale, e a rimetterci sono spesso le categorie con meno potere e che hanno meno visibilità nel discorso politico e sociale, prime fra tutte le donne.

Il problema della pornografia non consensuale

Il revenge porn, la **pornografia per vendetta**, è la diffusione di materiale pornografico senza il consenso della persona interessata per rovinare la sua reputazione e le sue relazioni sociali o, in alcuni casi, per ricattarla e sempre con il fine ultimo di vendicarsi di una relazione finita male, di un rifiuto o altre situazioni simili.

Secondo i dati di Eurispes, provenienti da un sondaggio dell'American Psychological Association, **il 90% delle vittime del revenge porn sono donne** e il fenomeno è talmente grave che il 51% delle persone interessate ha pensato al suicidio. Ecco perché alla luce di queste cifre non è possibile prendere alla leggera i deepfake porno. Le conseguenze per la vittima possono essere disastrose, soprattutto per le donne non famose. Come diceva Scarlett Johansson, il pubblico la conosce ed è difficile che credano all'autenticità dei deep fake porno che girano su Internet e che la vedono protagonista.

Tuttavia, questo discorso non vale per l'ex ragazza o la collega di lavoro di turno, e la diffusione di deepfake porno nel suo circolo sociale o tra i suoi contatti online può avere un impatto molto forte sulla sua vita. C'è chi se la cava con una discussione in famiglia, ma c'è anche chi si vergogna di farsi vedere a scuola o in città e addirittura chi perde il lavoro o non riesce a trovarne uno a causa della sua nuova "cattiva reputazione".

Cosa fare contro i deepfake porno

Le app come DeepNude e questo bot di Telegram potranno anche essere rimosse, ma ci sarà sempre qualcuno pronto a ripubblicarle in un altro formato o canale. La soluzione più efficace richiede impegno e sensibilità:

- Per prima cosa, **prendiamo coscienza dei deepfake** e impariamo a diffidare di foto e video porno di persone che conosciamo, perché quasi sicuramente non sono veri.
- Se anche lo fossero, noi non eravamo tra i destinatari autorizzati a riceverli, per cui dobbiamo **cancellare questi contenuti e segnalarli** alla piattaforma su cui sono stati diffusi.