l'Intervista

ATTENZIONE AI NOSTRI DATI ONLINE

A **RENATO PIZOLLI,** TENENTE E PORTAVOCE DELLA POLIZIA CANTONALE

Nel dicembre 2024, il Consigliere agli Stati del Centro **Fabio Regazzi** ha presentato una mozione al Consiglio federale, chiedendo l'elaborazione di una strategia coordinata per contrastare l'uso abusivo delle immagini e il ricatto tramite immagini intime, con un'attenzione particolare alla protezione di bambini e giovani. L'avanzamento dell'Intelligenza Artificiale (IA) ha reso possibile manipolare delle immagini innocue reperite online, trasformandole in contenuti falsi, spesso di natura sessuale. Questo fenomeno, noto come *deepfake*, viene frequentemente utilizzato a fini manipolatori e coercitivi: per ricatti monetari o per estorcere immagini sessualmente esplicite. La creazione e la diffusione dei *deepfake* sta diventando sempre più comune, rappresentando una nuova sfida nell'ambito della ciberstrategia. A questo riguardo abbiamo deciso di intervistare **Renato Pizolli**, tenente e portavoce della Polizia cantonale.

In base alle statistiche più recenti, quanti sono in Ticino i casi riconducibili alla cibercriminalità? Quali sono le principali forme di questo fenomeno? Ha notato un incremento nelle segnalazioni alla polizia per questo genere di reati?

I dati relativi al 2024 verranno pubblicati unicamente nella prossima primavera. Per quanto concerne il 2023 sono stati registrati 408 casi di criminalità digitale. I principali reati riscontrati in quest'ambito lo scorso anno sono stati:

- Abuso di identità e sistemi di pagamento personale ai fini di truffa;
- Pornografia vietata;
- Phishing;
- Cyberbullying e cybermobbing.

Le tipologie di truffa in questo ambito possono variare in base all'evoluzione dei metodi dei malfattori, che sono costantemente in adattamento. In generale, le segnalazioni a livello cantonale conoscono sul lungo periodo una certa stabilità, sebbene negli ultimi tempi si sia registrato un leggero aumento.

Anche alle nostre latitudini pare siano stati riscontrati casi di uso abusivo di immagini a fini ricattatori (*deepfake*). È così? O per ora ci siamo salvati da questo che appare essere divenuto un trend anche in Europa? Esistono casi che non emergono?

Non si può escludere che anche alle nostre latitudini si siano verificati abusi di immagini ai fini ricattatori, ma al momento non si registra alcuna denuncia. È importante sottolineare però che l'assenza di denunce non implica che questo modus operandi non sia presente sul nostro territorio, ma può essere dovuta alla paura delle vittime di essere giudicate o alla vergogna.

Il corpo di polizia è preparato alla gestione di questi casi? Mancano delle competenze o del personale adeguatamente formato? Come vengono gestite le segnalazioni in arrivo e in quale situazione viene aperta un'indagine?

La Polizia cantonale è preparata a gestire questo tipo di casistica, e non manca competenza in merito. Infatti, la Sezione analisi tracce informatiche (SATI) ha conosciuto un importante potenziamento delle competenze attraverso l'assunzione di profili professionali specializzati. Ogni segnalazione viene valutata con attenzione e vengono attivati i necessari accertamenti. Qualora vi siano concreti indizi di reato, e laddove necessario, dietro formale denuncia viene aperta un'inchiesta penale.

Quali sono i rischi che corrono i cittadini? Quali suggerimenti si sente di dare alla popolazione per evitare di incorrere in questo genere di reati?

I cittadini possono essere vittime di crimini informatici se non prestano attenzione nella gestione dei propri dati online.

Alcuni rischi comuni derivano da:
- Condivisione eccessiva di contenuti sensibili;
- Impostazioni di privacy non adeguate sui social media;
- Mancanza di autenticazione a due fattori;
- Password deboli o non modificate regolarmente.

Per proteggersi dalla sottrazione di dati personali, si consiglia di:
- Una sicurezza accresciuta per l'accesso indebito ai dispositivi;
- Non tenere la password scritta dietro il dispositivo stesso o nel portafoglio;
- Se a disposizione utilizzare strumenti di riconoscimento facciale;
- Monitorare il proprio nome e immagine online;
- Non cliccare link sconosciuti.

Per non incorrere in truffe, si consiglia di:
- Verificare sempre la fonte di un'informazione;
- Non lasciarsi ingolosire in offerte troppo allettanti o facili guadagni;
- Prima di investire consultarsi con specialisti o persone vicine.

Può fare un identikit del tipico criminale per questo genere di casi? Come agiscono?
La creazione di deepfake può essere compiuta sia da singoli individui che da gruppi criminali. Non esiste un «tipico criminale» per questo genere di reato, poiché con l'ausilio dell'intelligenza artificiale, è possibile creare contenuti senza una preparazione tecnica specifica. Le motivazioni più comuni sono il profitto e la manipolazione delle persone o delle situazioni.

Le vittime sono principalmente minorenni o adulti? Quali conseguenze riportano?
Poiché non disponiamo di dati dettagliati a livello cantonale, non possiamo fare una distinzione precisa. Tuttavia, le vittime di *deepfake* possono essere di tutte le età. Le conseguenze variano, ma in generale possono includere danni psicologici, danni reputazionali e, in alcuni casi, danni finanziari o emotivi a causa di molestie o ricatti.

Quali consigli si sente di dare ai genitori per proteggere i propri figli da potenziali minacce di questo tipo senza violare la loro privacy?
Si consiglia ai genitori di:
- Verificare e monitorare i livelli di privacy sui profili social dei figli;
- Sensibilizzare i giovani sull'importanza di limitare la condivisione di contenuti sensibili;
- Evitare l'uso eccessivo di selfie;
- Attivare l'autenticazione a due fattori su tutte le piattaforme online;
- Cambiare regolarmente le password e monitorare l'uso della propria immagine e del proprio volto online.

Ritiene necessario una maggior sensibilizzazione e prevenzione in questo ambito? In che modo secondo lei può essere efficace?
A vari livelli, in Ticino e in Svizzera, sono stati fatti numerosi sforzi in termini di sensibilizzazione e prevenzione. A livello cantonale, la polizia e altri enti collaborano attivamente per informare la popolazione riguardo ai rischi della criminalità digitale, mentre a livello nazionale, il NCSC (National Cyber Security Centre) e la Prevenzione svizzera della criminalità (PSC) hanno promosso diverse iniziative di sensibilizzazione.
È fondamentale continuare su questa strada, con una continua evoluzione delle strategie informative, preventive ed educative, per raggiungere non solo le persone più vulnerabili, ma anche sensibilizzare l'intera popolazione. L'efficacia di questi sforzi risiede nell'adozione di comportamenti preventivi quotidiani, come l'uso di strumenti di protezione online e la formazione continua sulla sicurezza informatica.

FS e FG