Internet non è un posto sicuro per donne e ragazze?

1 COMMENTO OFFENSIVO SU 10 RIVOLTO A UNA DONNA È SESSISTA

Le 150 parole più diffuse nei commenti offensivi, discriminatori o hate speech di matrice sessista.

«molestata da tre uomini»: Zuckerberg introduce la distanza di sicurezza fra avatar

Dopo l'episodio, accaduto all'interno di «Horizon Worlds», arriva la prima storica decisione da parte del social network

La comunicazione: gender gap nel linguaggio e commenti sessisti

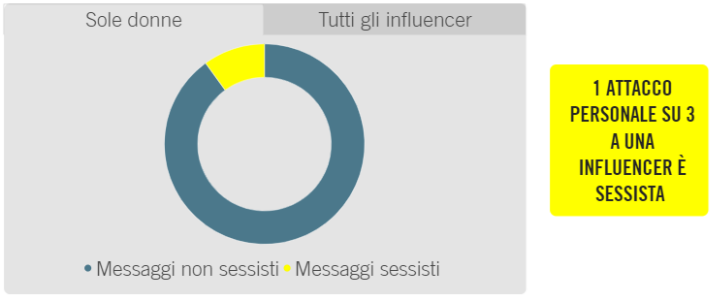
I RISULTATI

PIÙ DI 1 COMMENTO SU 10 È OFFENSIVO, DISCRIMINATORIO O HATE SPEECH

Che toni prevalgono nel dibattito online?

1 COMMENTO OFFENSIVO SU 10 RIVOLTO A UNA DONNA È SESSISTA

Attacchi sessisti sul totale dei commenti offensivi, discriminatori o hate speech.



1 COMMENTO OFFENSIVO SU 10 RIVOLTO A UNA DONNA È SESSISTA

Le 150 parole più diffuse nei commenti offensivi, discriminatori o hate speech di matrice sessista.

Mail Online Tennis

Home | News | Royals | U.S. | Sport | TV&Showbiz | Femail | Health | Science | Money | Travel | Shopping | Discounts

Football | Premier League | Transfer News | *Tennis* | Boxing | Six Nations | Racing | Cricket | Golf | F1 | MMA | US Sports | More | Login

Tennis star Matteo Berrettini splits from sex addict supermodel girlfriend Melissa Satta after 'very intense' year-long relationship

- **Italian tennis star Berrettini, 27, started dating Satta, 38, in January last year**
- **He has now confirmed they have split amicably despite a 'difficult' relationship**
- **She once confessed to having sex 'seven to ten times a week' with ex-husband Kevin-Prince Boateng**

By ADAM SHERGOLD
PUBLISHED: 13:22 GMT, 25 February 2024 | **UPDATED:** 15:23 GMT, 25 February 2024

Gli illeciti:
Dall'hate speech alla diffusione di immagini, al CYBERBULLISMO

Dati ed informazioni sui Social Network

Diffusione involontaria (ed illecita!)

- Phishing, furto di identità, furto e/o utilizzo fraudolento di dati
- Utilizzo illecito da parte dei gestori che hanno raccolto i dati per altre finalità
- Data Breach
- Altre ipotesi di illeciti tramite Internet

Illeciti on line

fattispecie in danno della persona

Flaming

Denigration

Outing

Trickery

Expoure

Impersonation

Exclusion

Hatespeech

Cybestalking

Cyberbashing

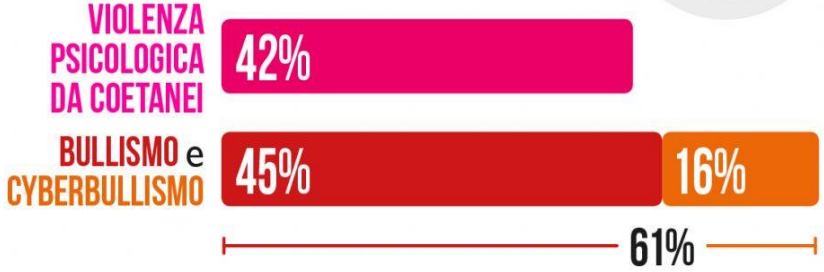
Sexting

Revenge porn

OSSERVATORIO indifesa

Indagine su un campione di 6.002 ragazzi dai 13 ai 23 anni, gennaio 2021

Hai mai **subito**: *(si poteva dare più di una risposta)*



Hai mai **assistito** ad atti di **bullismo e/o cyberbullismo?**

SÌ 68%

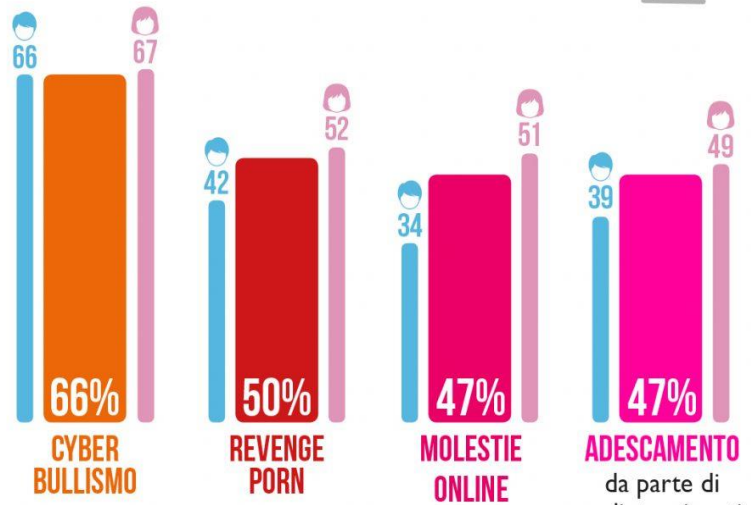
ScuolaZOO

Terre des hommes
Proteggiamo i bambini insieme

OSSERVATORIO indifesa

Indagine su un campione di 6.002 ragazzi dai 13 ai 23 anni, gennaio 2021

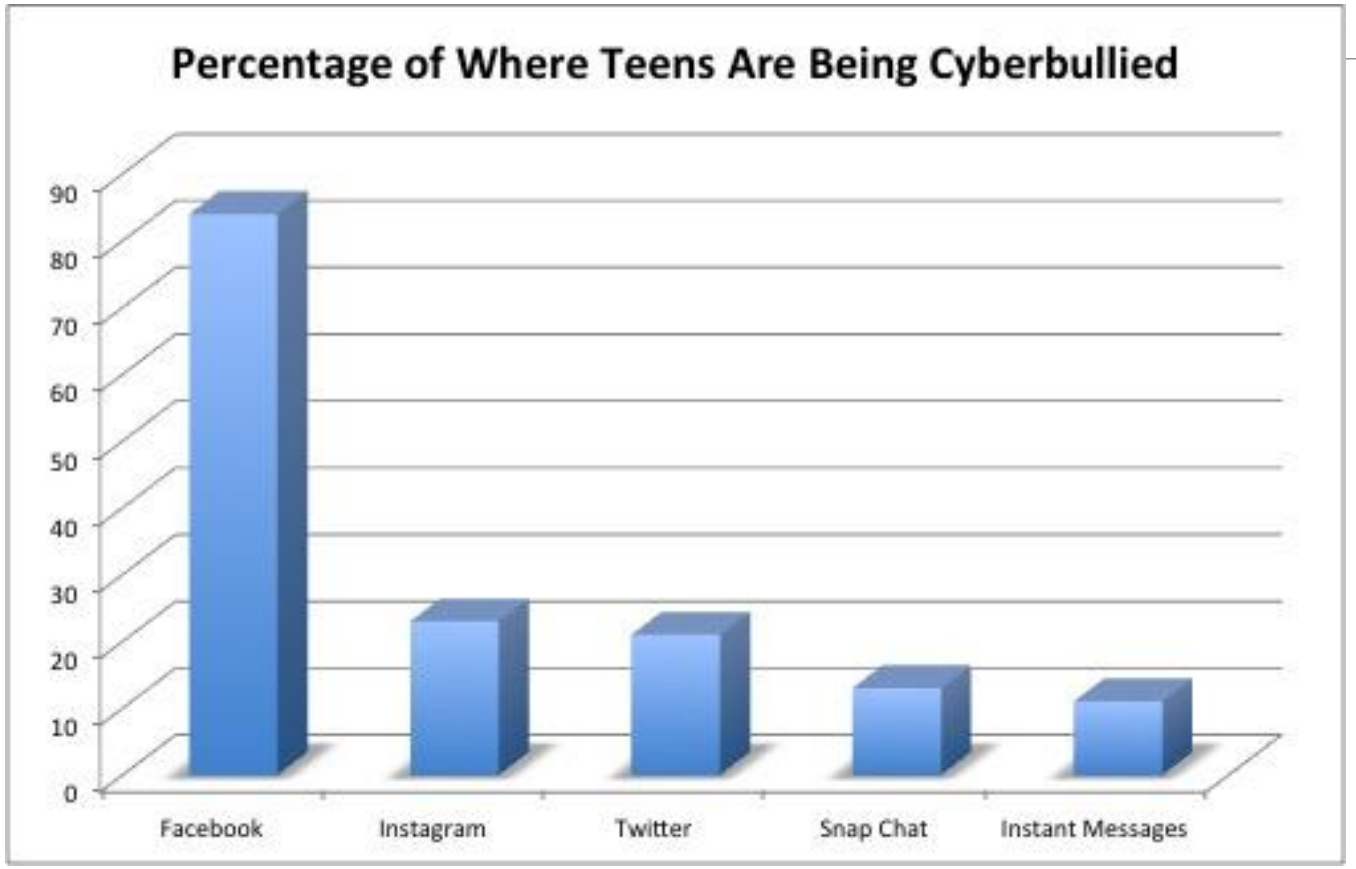
Qual è il rischio maggiore che un ragazzo/ragazza della tua età corre **online?**

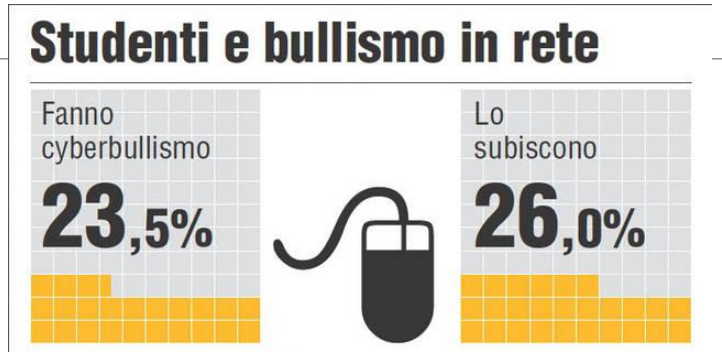


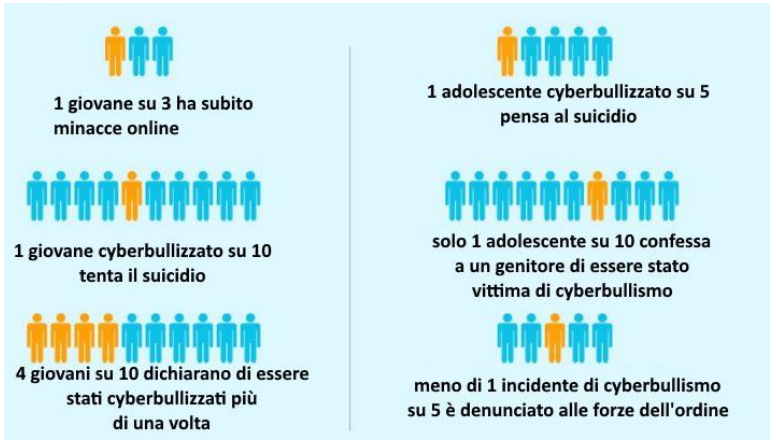
ScuolaZOO

Terre des hommes
Proteggiamo i bambini insieme

Social Network e diffusione del CyberBulling







Cyberbulling…..
ed altre ipotesi di illecito

Flaming

Denigration

Outing

Trickery

Expoure

Impersonation

Exclusion

Hatespeech

Cybestalking

Cyberbashing

Sexting

Revenge Porn

La legge 29 maggio 2017, n.71

Coniuga approccio preventivo e riparatorio

NON prevede nuove fattispecie a rilevanza penale, ma propone azioni per la tutela delle vittime e l'ammonimento dei «bulli»

Valorizza il ruolo delle Istituzioni Scolastiche

Definizione di cyberbulling (art.1)

qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.

alcuni punti critici….

Alcune condotte sono solo «fattuali», altre sono «normative»

Sembra porre in rilievo solo le condotte indirizzate all'isolamento…

Non prevede la reiterazione come carattere della condotta

Art. 2: notice and take down

Il minore vittima ultraquattordicenne o l'esercente la responsabilità genitoriale, può

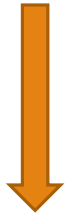
inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet, previa conservazione dei dati originali, anche qualora le condotte di cui all'articolo 1, comma 2, della presente legge, da identificare espressamente tramite relativo URL (*Uniform resource locator*), non integrino le fattispecie previste dall'articolo 167 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, ovvero da altre norme incriminatrici.

Destinatario della richiesta

Art. 1 comma 3

Ai fini della presente legge, per «gestore del sito internet» si intende il prestatore di servizi della società dell'informazione, diverso da quelli di cui agli articoli 14, 15 e 16 del decreto legislativo 9 aprile 2003, n. 70, che, sulla rete internet, cura la gestione dei contenuti di un sito in cui si possono riscontrare le condotte di cui al comma 2

ma il gestore di SN è host provider ex art.15



eppure rientra nella previsione dell'art.2 l.71/17

Richiesta di rimozione

Interessato inoltra al titolare trattamento o gestore sito o gestore social network

Entro 24 ore comunicazione ed entro 48 ore rimozione

Se non agisce ricorso all'AUTORITA' GARANTE PER IL TRATTAMENTO DEI DATI PERSONALI che agisce secondo la procedura ex legge 71/17 non con quella ex art.145 d.lgs.196/2003

Procedura di ammonimento (art.7)

Fino a quando non è proposta querela o non è presentata denuncia per taluno dei reati di cui agli articoli 594 (*depenalizzato*), 595 e 612 (*se grave perseguibile d'ufficio)* del codice penale e all'articolo 167 del codice per la protezione dei dati personali *(perseguibile d'ufficio)*, di cui al decreto legislativo 30 giugno 2003, n. 196, commessi, mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, è applicabile la procedura di ammonimento di cui all'articolo 8, commi 1 e 2, del decreto-legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla legge 23 aprile 2009, n. 38, e successive modificazioni.

Ammonimento ex legge 71/17 ed ammonimento ordinario

Presenza dei genitori

Non prevede sanzione in caso di reiterazione

Avviso di avvio procedimento

Fino ai 18 anni

In caso di reiterazione scatta la denuncia di ufficio

International Seminar

AIMED 2022

Economic and Policy Implications of Artificial Intelligence

Università Mediterranea di Reggio Calabria

Piattaforma Teams, 29- 30 settembre 2022

Deep Fake creazione, finalità rischi

«Fake - » e «Post realtà»

2017

Il Collins Dictionary indica la locuzione «fake news» come parola dell'anno

«false, often sensational information disseminated under the guise of news reporting»

Disinformazione

Echo chamber

Filter bubble

Diffusione di messaggi d'odio, delle notizie false ed alterazione del corretto percorso di formazione dell'opinione pubblica

Deep Fake

Manipolazioni

Video Audio Movimento

«tranelli cognitivi di conferma»

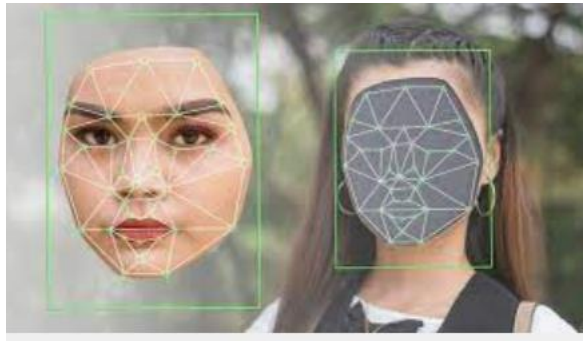
2017: **The Economist «fake news you ain't seen nothing**

2017: **Synthetizing Obama**

Creazione

Generative Adversarial Networks

Autoenconder



Face swap

Lip Syncr

Speech synthesis

Image-generation

sistemi open source
sistemi protetti da diritto di autore
sistemi «dark»

Finalità

Ludico – ricreativa

(app utilizzabili con minima alfabetizzazione informatica)

Cinematografia e documentaristica

Diffusione di contenuti falsi per alterare l'opinione pubblica

Diffusione di contenuti falsi contro un soggetto/gruppo

Cybercrime e frodi alle organizzazioni economiche


Rana Ayyub
her book
MY FACE WAS MORPHED
ON A PORN VIDEO: RANA AYYUB


RENXIT
CSU
960 × 540
Tagesschau
Visita
Manipulierte Videos: Auf dem Weg in eine alternative Realität? | tagesschau.de


Mikael Thalen
Twitter MikaelThalen
A deepfake of Ukrainian President Volodymyr Zelensky calling on his soldiers to lay down their weapons was reportedly uploaded to a hacked Ukrainian news website today, per
DEEPFAKE
La clip con il presidente ucraino
che invita il popolo a deporre le armi
0:55
NVITA ALLA RESA: IL FALSO VIDEO CREATO DAI RUSSI CON L'IA

Rischi

Malicious Use and Abuse of Artificial Intelligence (19.11.2020)

Perfezionare i reati di frode ed estorsione

Aggirare i sistemi di identificazione bancari

Falsificare documenti di identificazione

Falsificare le identità digitali

Perfezionare furti di identità o illeciti di «impersonificazione»

Realizzare attacchi reputazionali

Uso di AI e deepfake per finalità illecite

Spear Phishing

Vishing

Whaling

CEO fraud

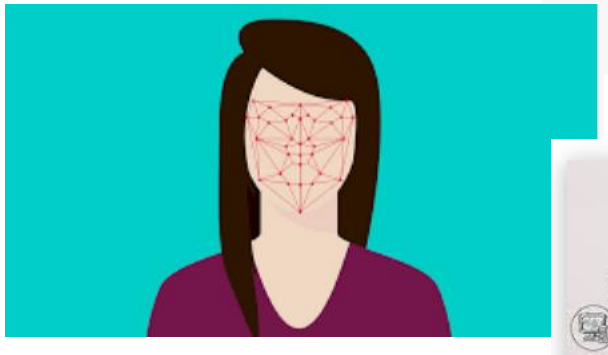
Face morphing

Face swipping

Voice mimicking

Deep nude

Cyberbullismo



Strumenti di tutela

Intervento normativo ad hoc?

Misure di sicurezza

Formazione/Prevenzione

Codici condotta per uso mail e social media

→ **Dicembre 2020: Vademecum Autorità Garante per il trattamento dei dati personali**

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 appare pixellata (cioè un pò "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, alla Polizia postale) o al **Garante per la protezione dei dati personali**.