LUISS

Dipartimento di Impresa e Management
Diritto di internet: social media e discriminazione

Distorsione digitale:
Analisi dell'alterazione dei contenuti online

Prof. Pietro Santo Leopoldo Falletta

RELATORE

Tommaso Agliata
258861

CANDIDATO

ANNO ACCADEMICO 2022 /2023

Dedicato alla mia famiglia.

Distorsione digitale: analisi dell'alterazione dei contenuti online

INDICE

Introduzione

La diffusione sempre più ampia e pervasiva delle tecnologie digitali ha portato a un notevole aumento della produzione e del consumo di contenuti online. Tuttavia, questa crescita esponenziale ha anche aperto la strada a una serie di problematiche, tra cui l'alterazione dei contenuti digitali.

L'alterazione dei contenuti online rappresenta un fenomeno complesso e in continua evoluzione che ha profonde implicazioni sociali, politiche ed economiche. La presente tesi si propone di analizzare l'alterazione dei contenuti online, le fake news e le sue varie manifestazioni, nonché le conseguenze economiche e legali che ne derivano.

Il primo capitolo affronta i caratteri generali dell'alterazione dei contenuti online. Si esplora il concetto di alterazione dei contenuti, concentrandosi sulle sfide che essa pone alla società contemporanea. Inoltre, si discute ampiamente delle fake news, un fenomeno in diffusione esponenziale che suscita grande preoccupazione in tutto il mondo per le sue possibili conseguenze sulla credibilità dell'informazione. Vengono quindi esaminate le cause alla base della produzione di fake news e gli effetti che queste hanno sulla disinformazione della società e si analizzano le fasi principali di creazione e diffusione di quest'ultime. Infine, si introduce l'idea che la tecnologia blockchain possa rappresentare una possibile soluzione per contrastare le fake news, fornendo trasparenza e tracciabilità alla produzione e alla diffusione dei contenuti online.

Il secondo capitolo si focalizza sugli esempi di alterazione dei contenuti online. Si esplora la disinformazione online, che comprende una vasta gamma di pratiche volte a manipolare l'opinione pubblica e a diffondere informazioni false. Uno degli esempi più inquietanti di alterazione dei contenuti digitali è rappresentato dai deepfake, che sono video o audio manipolati in modo da sembrare autentici ma che in realtà sono completamente falsi. Vengono presentati esempi concreti di deepfake e si discute delle implicazioni che essi hanno sulla fiducia nell'informazione e sull'integrità dei media. Inoltre, si esamina la manipolazione di immagini online, la creazione di siti web falsi e la modifica di post sui social media come ulteriori manifestazioni dell'alterazione dei contenuti digitali. Infine, si affronta il tema della manipolazione dei motori di ricerca e si esplora l'aspetto economico del cybercrime, che rappresenta una delle economie illegali più redditizie a livello globale.

Il terzo capitolo si concentra sulle conseguenze economiche e legali dell'alterazione dei contenuti online. Si analizza l'impatto economico che l'alterazione dei contenuti digitali ha sulle aziende, sui settori industriali e sull'economia nel suo complesso. Vengono esplorate le implicazioni finanziarie della diffusione di fake news e della manipolazione dei contenuti online. Inoltre, si esaminano le varie conseguenze legali dei reati di alterazione dei contenuti digitali, con particolare attenzione al contesto italiano.

Capitolo 1
L'ALTERAZIONE DEI CONTENUTI ONLINE

1.1 Caratteri generali dell'alterazione dei contenuti online

Tra i principi fondamentali di ogni sistema democratico vi sono la libertà e la credibilità dell'informazione, che rappresentano, a loro volta, l'essenza stessa dell'attività di informazione pubblica e del giornalismo, il cui primo dovere è nei confronti della verità.

Nel corso dei secoli le modalità con cui veicolare le notizie si sono evolute sino a cambiare radicalmente: dalla pressa a caratteri mobili di Johannes Gutenberg, che diede avvio alla stampa moderna, alla radio, alla televisione per arrivare alla rete internet dei nostri giorni. Ogni nuovo mezzo di comunicazione ha sempre rappresentato un enorme passo avanti e allo stesso tempo una sfida per l'impatto sulla società, con conseguenti ricadute anche in termini di responsabilità degli operatori del settore.

Il Legislatore è sempre intervenuto, con normative specifiche di settore come, ad esempio, le leggi sulla radio e sulla televisione, al fine di cercare di impedire abusi, garantire il pluralismo e, soprattutto, tutelare i cittadini a cui i media si indirizzano.

Al giorno d'oggi, la possibilità di essere informati costantemente e in tempo reale su quanto accade nel mondo rende internet uno strumento meraviglioso e finanche imprescindibile, in grado di annullare le distanze e di fornire una mole di dati ed informazioni del tutto impensabile sino a pochi anni or sono.

Il web ha sicuramente rappresentato la più grande rivoluzione degli ultimi tempi, non solamente sotto l'aspetto tecnologico, ma anche sociale e culturale; la rete di internet ha infatti permesso di accedere ad informazioni infinite riducendo le distanze tra classi sociali e consentendo, nei Paesi oppressi da regimi totalitari, la denuncia di atroci crimini che, senza internet, sarebbero rimasti sconosciuti all'opinione pubblica.

Non per nulla alcuni tra questi Paesi, consapevoli delle potenziali ripercussioni che la diffusione di notizie di tal genere avrebbe potuto causare, hanno cercato con alterne fortune di vietare o limitare l'uso della rete, oppure di filtrare le notizie da essa veicolabili, ponendo

in atto una sorta di moderna censura governativa.

Grazie alla velocità, da un lato, e alla pervasività, dall'altro, la rete ha dunque messo a conoscenza l'opinione pubblica mondiale di quanto accade in luoghi lontani e tradizionalmente “chiusi” sia nell’informare la propria cittadinanza dei fatti del mondo esterno che nel far trapelare i propri accadimenti interni; d’altro canto, purtroppo, il mondo di Internet ha però mostrato nel corso degli anni di possedere anche un suo lato oscuro, tanto da far emergere i «pericoli del web» e da dover mettere a punto una «netiquette» per il rispetto degli utenti.

Nell'era dell'informatizzazione di massa e dell’uso quotidiano da parte di milioni di utenti delle risorse messe a disposizione dal web, appare di piena evidenza la gravità del danno che la diffusione di una notizia errata, falsa o distorta, se non addirittura volutamente manipolata, può comportare.

Le notizie false, o fake news o “bufale”, ci sono sempre state, ma chiaramente non si sono mai diffuse e propagate con la velocità attuale.

Quando, poi, l'informazione diventa disinformazione i mezzi di comunicazione di massa possono essere strumentalizzati per influenzare l'opinione pubblica, anche perché con il diffondersi dei social media il pericolo di contaminare internet con notizie inesatte e infondate è in crescita esponenziale.

Da qui, è opportuno soffermarsi sul concetto stesso di «notizia». Un concetto che è sicuramente mutato nel passaggio dai media tradizionali ai social media e alle piattaforme online, colme di contenuti generati dagli utenti, dove si è imposto l'«infotainment», vale a dire la mescolanza d'informazione e intrattenimento, tipicamente sfruttabile a fini commerciali.

Ma il rischio tra la mancata distinzione di notizie frutto di una competenza giornalistica e notizie diffuse sul web senza alcun criterio professionale risiede proprio qui: chiunque, infatti, può dire quello che vuole, per la più che legittima libertà di espressione, ma se il pubblico di internet prende per buono e fondato qualsiasi notizia o opinione circoli online, senza più distinguere tra vero e falso e senza essere in grado di verificare la correttezza e l’autorevolezza della fonte, il pericolo è enorme.

In particolar modo quando i temi trattati riguardano aspetti sensibili della società come, per esempio, la sanità e soprattutto se le opinioni si mescolano in maniera indistinta ai fatti.

Oggi, del resto, sembra che la disinformazione prevalga sull'informazione oggettiva e che la manipolazione e la propaganda abbiano la meglio sulla corretta espressione delle proprie opinioni e punti di vista.

Spesso viene superata la linea che separa ciò che potrebbe essere considerato un tentativo legittimo di esprimere le proprie opinioni a scopo persuasivo e quella che è invece disinformazione e manipolazione. [1]

1.2 Le fake news

1.2.1 Cosa sono le fake news

L'Enciclopedia Treccani definisce il termine Fake News così: "*fake news ovvero locuzione inglese (lett. notizie false) entrata in uso nel primo decennio del XXI secolo per designare un'informazione in parte o del tutto non corrispondente al vero, divulgata intenzionalmente o non intenzionalmente attraverso il Web, i media o le tecnologie digitali di comunicazione, e caratterizzata da un'apparente plausibilità, quest'ultima alimentata da un sistema distorto di aspettative dell'opinione pubblica e da un'amplificazione dei pregiudizi che ne sono alla base, ciò che ne agevola la condivisione e la diffusione pur in assenza di una verifica delle fonti*".[2]

L'espressione "*fake news*" può quindi essere utilizzata indistintamente per indicare molti concetti tutti riconducibili a vario modo a "disturbi dell'informazione" che generano nell'individuo e nella collettività disinformazione. Possiamo annoverarvi:

- notizie provenienti da fonti non verificate;

1 Fonte: Disegno di legge n.2688 Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica.

[2] Origine storica del termine Fake News: *"Il termine Fake News è certamente un neologismo, ma il concetto di falsa notizia è tutt'altro che nuovo. Pare infatti che Augusto, primo imperatore di Roma, condusse una vera e propria campagna di disinformazione contro il rivale Marco Antonio, accusato di essere un ubriacone e burattino al soldo di Cleopatra. In balia di tali dicerie e a seguito della notizia (falsa anch'essa) che Cleopatra si fosse suicidata, Marco Antonio si tolse la vita. Grazie a una fake news, Augusto era riuscito a distruggere la Repubblica e ad instaurare l'Impero"*. [Fonte: "Libertà di espressione online e Fake News", alla luce del Diritto Costituzionale e del Diritto Europeo - Ius in itinere]

- notizie satiriche che possono essere percepite come reali;
- notizie provenienti da fonti che alimentano teorie complottistiche o cospirazioniste;
- notizie provenienti da fonti specializzate in pettegolezzo;
- hate news provenienti da fonti che promuovono razzismo, misoginia, omofobia, e altre forme di discriminazione;
- notizie (del tutto o parzialmente) corrette che però utilizzano un titolo sensazionalistico per attirare l'attenzione (a scopi di clickbaiting – cattura dei click);
- notizie provenienti da fonti che forniscono, in maniera tendenziosa, informazioni a supporto di specifici punti di vista e orientamenti politici.[3]

È bene precisare che la nozione di *fake news* non include le informazioni e le notizie che sono già vietate per effetto di altre norme "tipiche", come ad esempio quelle sulla diffamazione, sull'incitazione a delinquere o sulla propaganda razzista.

1.2.2 Perché si producono le fake news e gli effetti sulla disinformazione

Le fake news possono circolare per vari motivi con l'obiettivo, comunque, di influenzare intenzionalmente il pensiero del destinatario. Queste possono essere di natura economica (es. clickbait) con lo scopo di realizzare profitti con la pubblicità rivolta a chi naviga sui siti web ove la notizia è pubblicata[4] o di natura politica (o ideologica) al fine di influenzare l'opinione pubblica.

Generalmente chi produce fake news, a differenza dei fornitori tradizionali di informazioni, non si preoccupa di produrre e diffondere notizie accurate e non tenta di costruirsi una buona reputazione, ma intende solo massimizzare i guadagni derivanti dai click ricevuti sulla singola falsa notizia o manipolare l'informazione al fine ultimo di creare uno scontro politico o ideologico[5] o per fini commerciali[6].

3 Fonte: RAPPORTO AGCOM: Le strategie di disinformazione online e la filiera dei contenuti fake

4 Ad esempio, gli adolescenti di Veles, che hanno prodotto fake news sia a favore di Donald Trump che di Hillary Clinton, in occasione delle elezioni presidenziali del 2016 hanno guadagnato decine di migliaia di dollari. Paul Horner ha dichiarato di aver creato fake news a favore di Trump per ricavare profitti nonostante sostenesse di essere personalmente un suo oppositore.

[5] Soprattutto durante le campagne elettorali, le parti politiche utilizzano le fake news che possano mettere in cattiva luce alcuni membri della controparte o l'ideologia intera degli avversari. Poco importa se tali notizie siano fondate o meno, ciò che importa è che abbiano un impatto emotivo sugli elettori.

Proprio in virtù delle loro caratteristiche le fake news sono particolarmente diffuse sui social networks, il luogo per eccellenza dell'interazione sociale dove è possibile trovare un pubblico eterogeneo in base all'età, alla formazione culturale e ideologica, agli interessi e alle abitudini.

I social media hanno, infatti, favorito la diffusione di storie false facendo spesso leva sulle emozioni per attirare l'attenzione. Per questo anche le persone giovani e con competenze digitali possono avere difficoltà a identificare le notizie che sono state manipolate.

Le piattaforme dei social media sono diventate un terreno fertile per la diffusione delle fake news. Queste piattaforme si basano su algoritmi[7] che danno priorità al coinvolgimento e le fake news vengono spesso condivise più delle notizie vere a causa della loro natura sensazionalistica. Su Twitter, ad esempio, le fake news si diffondono più rapidamente rispetto alle notizie vere e hanno il 70% di probabilità in più di essere retwittate.

Secondo un sondaggio condotto dal Censis[8] nel 2020, solo il 42,8% degli italiani considera i siti web d'informazione credibili. Prevale quindi il giudizio negativo: per il 57,2% sono poco o per nulla attendibili mentre, per quanto concerne i social network, essi sono ritenuti non del tutto affidabili dal 66,4% degli italiani.

Nella tendenza alla perdita di fiducia spiccano i media digitali. Nell'ultimo anno gli utenti hanno cominciato a vedere queste piattaforme come veicoli di notizie soggette a possibili manipolazioni. Il risultato è che il 27,2% degli italiani si fida di meno dei social network e il 20,7% ha meno fiducia nei siti d'informazione online.

Inoltre, secondo l'osservatorio sulle fake news della Fondazione Bruno Kessler, nel 2020 il 18% delle notizie condivise dagli utenti sui social media in Italia erano false o manipolate.

Un'altra fonte di dati sulle fake news in Italia è l'organizzazione di fact-checking Pagella Politica, che nel 2020 ha verificato circa 600 notizie, di cui il 58% sono risultate false o fuorvianti.

Il problema legato alla diffusione delle fake news riguarda proprio l'impatto che esse generano sulle scelte individuali, fino a rappresentare in certi casi un vero pericolo per il

[6] Significativo è il fenomeno della diffusione di false recensioni su piattaforme come Tripadvisor costruite ad hoc per screditare le attività imprenditoriali dei concorrenti o, al contrario, scritte dai proprietari stessi dei locali attraverso profili falsi per esaltarne le qualità.

[7] Algoritmo: Un procedimento di calcolo esplicito e descrivibile con un numero finito di regole che conduce ad un risultato dopo un numero finito di calcoli. Non è mai completamente neutro, in quanto ci sono elementi di filtraggio.

[8] Il Censis è un istituto di ricerca socioeconomica italiano fondato nel 1964

benessere personale e collettivo. La loro diffusione ha il fine ultimo di orientare le scelte delle persone in certe precise direzioni e rafforzare le idee su determinate tematiche, con l'intenzione dichiarata di crearne di nuove o di contribuire ad alimentare teorie talvolta complottistiche o "antisistema".

La presenza di fake news ha quindi diverse implicazioni negative sul benessere sociale.

Nell'era digitale la divulgazione delle fake news e la conseguente disinformazione è un fenomeno pervasivo molto più efficace e difficile da individuare rispetto al passato, proprio perché gli strumenti di diffusione cambiano rapidamente e soprattutto perché manca il giusto spirito critico dell'interlocutore, che sempre più di frequente recepisce le informazioni senza avere idea di quale sia la fonte e di quanto siano attendibili.

In più il desiderio di esser parte dell'universo social fa sì che oggigiorno le persone siano non più solo fruitori, ma anche fonte dell'informazione stessa che circola nel web, attraverso la condivisione, la distorsione e la creazione di notizie.

Questo doppio ruolo rende fondamentale saper utilizzare nel modo giusto la Rete. E' necessario imparare a verificare i fatti e l'attendibilità delle fonti, a carpire la differenza tra siti di informazione affidabili o meno e soprattutto bisogna educare la collettività al principio della responsabilità individuale delle notizie condivise.

Se è pur vero che la libertà di espressione deve essere sempre difesa, è altresì fondamentale garantire il diritto ad un'informazione corretta ed attendibile.

Ed è proprio con l'obiettivo di favorire la diffusione di una corretta informazione che è opportuno attenersi ad alcune utili regole di condotta per difendersi dalle fake news:

1. Controllare la notizia: verificare su Internet se la notizia è riportata da altre fonti di riconosciuta autorevolezza e se il contenuto non sia già stato etichettato come bufala. Un processo di fact-checking ottimale dovrebbe consentire di reperire la medesima notizia in almeno altre 4/5 testate giornalistiche registrate.
2. Controllare l'indirizzo del sito: la URL del sito può rivelare il proprio grado di autorevolezza. Per capire la veridicità della url può esser utile verificare la sezione "chi siamo?" per capire chi c'è dietro e chi finanzia il sito stesso.
3. Controllare l'autore: verificare che chi produce e diffonde la notizia sia davvero un esperto realmente accreditato.
4. Controllare le fonti: se l'autore usa fonti affidabili e note.

5. Controllare le immagini: le immagini hanno grande forza e sono facilmente manipolabili. Effettuando una ricerca per immagini è possibile vedere se un'immagine è già stata utilizzata in un contesto diverso.
6. Riflettere prima di condividere: se leggiamo una notizia particolarmente sensazionalistica o incredibile, poniamoci questa domanda: "Ma è davvero possibile?". È necessario sviluppare senso critico, che può aiutarci ad essere utenti sempre più consapevoli e a non diventare complici di chi dissemina disinformazione.

Se si considera il complesso delle distorsioni dell'informazione online, le motivazioni che spingono gli ideatori dei contenuti fake sono numerose, di natura svariata e spesso non univoche. Si possono distinguere essenzialmente:

1. Motivazioni economiche, di breve-medio periodo (finalizzate al recupero di risorse economiche dalla pubblicità e/o da azioni fraudolente) e di lungo periodo (finalizzate al recupero di risorse economiche attraverso strategie varie che puntano, per esempio, al discredito di imprese concorrenti o a influenzarne il valore sui mercati finanziari).
2. Motivazioni ideologico-politiche.
3. Motivazioni psicologiche, legate alla volontà del singolo di affermarsi nelle comunità online.
4. Motivazioni ludico-satiriche.

Si può altresì osservare come le motivazioni di ordine economico e politico-ideologiche spesso si intreccino e coesistano all'interno di un'unica strategia, così che non è sempre agevole distinguere i reali obiettivi degli ideatori di una campagna di disinformazione.

1.2.3 Le fasi principali di una fake news

Si possono distinguere quattro fasi principali che costituiscono la filiera dei contenuti fake online: una prima fase di creazione del messaggio; una seconda fase di produzione del contenuto in cui il messaggio viene trasformato in un prodotto informativo; una terza fase di distribuzione del contenuto; una quarta in cui i contenuti fake sono infine valorizzati.

Nella prima fase di creazione, viene elaborato il messaggio da trasmettere mediante il contenuto fake; questo assume caratteristiche diverse in ragione dell'obiettivo degli ideatori e a seconda del target cui è destinata la strategia di disinformazione.

In generale, per risultare efficace, il messaggio deve essere costruito in maniera tale da raggiungere l'audience e coinvolgendola anche nella diffusione del contenuto; a questo fine, si evidenziano alcuni elementi fondamentali, che sono:

-Il profilo degli utenti e il target di riferimento: l'accuratezza della profilazione degli utenti online permette di predisporre messaggi e contenuti fake più efficaci rispetto all'audience target; in fase distributiva consente una diffusione mirata dei contenuti incrementando l'efficacia della campagna di disinformazione.

-L'analisi del contesto e la scelta dei temi trattati nel messaggio: presuppone un'analisi dei temi "caldi" che circolano sul web all'interno di determinate comunità, così da individuare quelli su cui è più probabile focalizzare l'attenzione e favorire così la diffusione del contenuto fake. Tali temi dipendono dal contesto economico, sociale, politico, e più in generale culturale, in cui il target di riferimento si colloca. Inoltre, essi variano nel tempo, anche piuttosto rapidamente, per cui si rende utile un loro monitoraggio continuo.

-Il modo in cui gli individui elaborano le informazioni: il contenuto dovrebbe soddisfare non solo i bisogni di informazione, ma soprattutto le aspettative dei destinatari in termini di corrispondenza rispetto alle proprie convinzioni, di coinvolgimento emotivo e di condivisione della visione del mondo. I contenuti dei messaggi facenti parte di campagne di disinformazione dovrebbero quindi soddisfare (e sfruttare) le tendenze degli utenti a leggere e condividere informazioni conformi al loro punto di vista e di potenziale interesse all'interno delle echo chambers[9] in cui si struttura un'opinione pubblica sempre più polarizzata.

In particolare, questi aspetti (target, contesto e processi cognitivi) incidono sulla scelta del codice della comunicazione, quindi sia sul linguaggio per la composizione del messaggio (parole, immagini, suoni), sia sul modo in cui il messaggio è inquadrato. La considerazione congiunta dei tre elementi, dunque, porta alla definizione di messaggi con specifiche caratteristiche e una precisa struttura.

Nella seconda fase di produzione del contenuto, il messaggio viene trasformato in un prodotto informativo, che può assumere la forma di un testo (ad esempio, un post o un

[9]Echo chambers: Treccani: Nella società contemporanea dei mezzi di comunicazione di massa, caratterizzata da forte interattività, situazione in cui informazioni, idee o credenze più o meno veritiere vengono amplificate da una ripetitiva trasmissione e ritrasmissione all'interno di un ambito omogeneo e chiuso, in cui visioni e interpretazioni divergenti finiscono per non trovare più considerazione.

articolo), di un'immagine, di un video, oppure una combinazione di questi elementi.

In questa fase si possono rinvenire diversi "generi" di contenuti fake che possono essere osservati da molteplici punti di vista. Ad esempio, in base al grado di "manipolazione" del messaggio, idealmente, si va dal contenuto completamente falso, quindi fabbricato ex novo, a quello basato su un'informazione originaria vera ma manipolata.

La manipolazione può riguardare il messaggio contenuto (contenuti manipolati), le informazioni di contesto (false contestualizzazioni), il titolo, le immagini, o le didascalie (false connessioni), la fonte; si arriva fino ai contenuti parodistici e satirici oppure fuorvianti, in cui la manipolazione può riguardare l'inquadramento del messaggio.

In particolare, una pratica comune nel mondo online, e che si osserva anche nell'ambito dei contenuti fake, è l'adozione di un codice comunicativo al confine tra comunicazione commerciale e comunicazione informativa. È il caso, ad esempio, dei contenuti di disinformazione sponsorizzati e dei dark ads[10] che sfruttano le tecnologie che consentono una personalizzazione dei messaggi veicolati nell'ambito del sistema di diffusione della pubblicità online.

Nella terza fase di distribuzione, il contenuto fake viene pubblicato online e reso quindi disponibile. In questa fase si decide il canale distributivo (o i canali distributivi) e il contesto mediatico in cui il contenuto si inserisce. Il primo può essere tipicamente un sito web (ad esempio il sito di un editore online, una piattaforma social, un blog, un forum, etc.) oppure un'applicazione (ad esempio di instant messaging). In genere, questi strumenti sono un canale preferenziale, principalmente perché rendono più facile mantenere l'anonimato e costituiscono una modalità di distribuzione con costo praticamente pari a zero.

Il contesto mediatico rappresenta, invece, la rete di contenuti (testi, immagini, suoni) che circola sui diversi media online e offline; in particolare, nella fase distributiva si definisce il contesto mediatico che si colloca attorno ai contenuti fake, che è importante soprattutto per conferire attendibilità al messaggio.

Nell'ultima fase, la quarta, i contenuti fake vengono valorizzati, ossia possono produrre guadagni monetari più o meno immediati attraverso l'adozione di una serie di strategie commerciali, oppure possono raggiungere gli scopi desiderati senza generare

[10] Dark ads: La pubblicità oscura è un tipo di pubblicità online visibile solo all'editore dell'annuncio e al gruppo target previsto.

necessariamente un flusso di entrate monetarie, poiché rispondono ad altre motivazioni.
In particolare, per ciò che riguarda i ricavi, soprattutto in strategie commerciali di breve-medio periodo, esistono due fonti principali di remunerazione per i produttori: le risorse pubblicitarie e, in alcuni casi, il contributo diretto degli utenti ottenuto con azioni fraudolente.
Nell'ambito di strategie di più lungo periodo, ritorni economici possono derivare ad esempio da campagne di disinformazione che, danneggiando l'immagine e la reputazione di un'impresa concorrente, mirano a sottrarre quote di mercato.
Infine, si riscontra la presenza di strategie ibride, in cui coesistono finalità politico-ideologiche e finalità di natura economica, che possono produrre un'alterazione degli assetti di un mercato, tale da determinare un rafforzamento della posizione economica di alcuni soggetti d'impresa a scapito di altri, generando così dei vantaggi economici per gli ideatori.

1.3 Blockchain, una possibile nuova soluzione contro le fake news

Una soluzione efficace per contrastare la disinformazione potrebbe essere offerta proprio dalla tecnologia, in particolar modo dalla blockchain.
La blockchain, infatti, basa il suo funzionamento sulla Distributed Ledger Technology (DLT)[11], ovvero una tecnologia creata su un registro distribuito e su criteri come trasparenza, tracciabilità e sicurezza. Per queste peculiarità può essere utilizzata per aumentare la fiducia e la trasparenza in tutta la catena di approvvigionamento delle materie prime - nel nostro caso delle fonti -, aiutando a riconciliare la documentazione e i dati richiesti per certificare la qualità del "prodotto" finale.
Chiamata per l'appunto anche tecnologia della fiducia, la blockchain in questo modo garantisce anche che qualsiasi tipo di transazione sia memorizzata e convalidata da tutti i partecipanti alla "catena di blocchi" in modo da diventare immutabile.

[11] Con il termine Distributed Ledger Technologies *(*DLT*)* si fa riferimento a "libri mastri" (o registri) elettronici, distribuiti geograficamente su un'ampia rete di nodi, i cui dati sono protetti da potenziali attacchi informatici grazie al fatto che le stesse informazioni sono ridondate, verificate e validate mediante l'adozione di diversi protocolli (o regole) comunemente accettati da ciascun partecipante. Fonte: Technology Distributed Ledger, Ministry of Enterprises and made in Italy.

Per quanto riguarda la disinformazione, dunque, essa potrebbe contribuire a rendere noto l'autore e la sua attendibilità, assicurarsi che i vari contenuti da una fonte all'altra non subiscano alterazioni non autorizzate, incentivare la creazione di contenuti che soddisfino gli standard guidati dalla comunità per quanto concerne accuratezza e integrità.

Sono essenzialmente due gli studi che si stanno concentrando sulla possibilità di rendere la blockhain un nuovo metodo per contrastare le fake news, uno dei quali inserito nel progetto Feedback Analysis and Blockchain-based trust Evaluation (FAKE).
A fronte dei possibili vantaggi, permangono alcuni punti interrogativi, ad esempio, sui contenuti utilizzati per valutare il contenuto di una notizia. Alcuni criteri usati per la segnalazione di fake news, infatti, potrebbero non essere considerati universalmente validi e chiamati a fronteggiare il continuo cambiamento nel mondo dell'informazione.

Come spesso accade in questi casi, solo il tempo sarà in grado di rivelare l'effettivo impatto che potrà avere la tecnologia blockchain sul mondo della disinformazione e sul contrasto alla proliferazione delle fake news.

CAPITOLO 2

ESEMPI DI ALTERAZIONE DI CONTENUTI ONLINE

Di seguito sono riportati alcuni esempi di alterazione dei contenuti online e le relative implicazioni.

-*Disinformazione online*: essa può essere utilizzata per diffondere idee false con l'intento di ingannare o manipolare i lettori.

-*Deepfake*: consente di creare media digitali realistici che sembrano reali ma in realtà sono completamente fabbricati.

-*Manipolazione di immagini online*: essa può essere utilizzata per creare falsi video o fotografie che sembrano autentiche, ma che in realtà non lo sono. Ciò può essere fatto per diffondere disinformazione, screditare qualcuno o per scopi politici.

-*Modifica di post sui social media*: la modifica di post sui social media può essere utilizzata per cambiare il significato del messaggio originale o per diffondere informazioni false, ad esempio per influenzare l'opinione pubblica su un determinato argomento.

-*Creazione di siti web falsi*: la creazione di siti web falsi può essere utilizzata per diffondere informazioni false o per trafugare dati personali. Ad esempio, i truffatori possono creare siti web falsi di banche o società di carte di credito per raccogliere informazioni personali e finanziarie.

-*Spamming di recensioni online*: utilizzato per influenzare l'opinione degli utenti sui prodotti o servizi di un'azienda. Tale pratica può essere posta in essere da concorrenti sleali o da aziende che cercano di migliorare la loro reputazione online.

-*Manipolazione dei motori di ricerca*: la manipolazione dei motori di ricerca può essere utilizzata per posizionare i propri contenuti in cima ai risultati di ricerca. Ciò può avvenire attraverso tecniche di SEO sleali o tramite l'acquisto di link di ritorno.

2.1 Disinformazione online

Nel caso in cui la manipolazione dei contenuti informativi online sia caratterizzata tanto da falsità che dall'intento doloso ci si può riferire alla nozione di disinformazione.

In questa categoria sono incluse tutte quelle informazioni false (ma suscettibili di essere recepite come vere), deliberatamente create per danneggiare, anche grazie all'impatto

emotivo, una persona, un gruppo sociale, un'organizzazione o un Paese, o affermare/screditare una tesi, e consapevolmente diffuse per scopi politici, ideologici o commerciali (incluso il clickbaiting[12]), quasi sempre attraverso piattaforme online che tendono ad aumentarne la propagazione massiva. Si tratta, infatti, di contenuti contraddistinti da viralità in base all'argomento trattato, a trasferire stati emotivi e percezioni su larga scala. Nello specifico, sono riconducibili a questa tipologia fenomeni quali false contestualizzazioni (che si verificano quando contenuti veritieri sono condivisi con false informazioni di contesto), contenuti veicolati da false fonti (contenuti divulgati da fonti false che impersonano fonti autentiche), contenuti creati in maniera artificiosa (contenuti totalmente falsi e infondati creati per ingannare e/o danneggiare), notizie manipolate (informazioni o immagini veritiere manipolate in modo volutamente ingannevole).

L'avvento di Internet e dei social media ha rivoluzionato il modo di comunicare, raccogliere informazioni e condividere notizie, ma ciò ha portato anche alla diffusione della disinformazione online. Essa può essere diffusa attraverso vari mezzi, tra cui social media, blog, siti web e piattaforme di messaggistica.

Le origini della disinformazione possono essere fatte risalire agli albori della propaganda, utilizzata da governi e organizzazioni politiche per manipolare l'opinione pubblica.

L'uso della propaganda è continuato per tutto il XX secolo, con la sempre maggiore divulgazione dei mass media[13] e lo sviluppo di nuove tecnologie come la radio e la televisione.

Tuttavia, al giorno d'oggi sono stati Internet e i social media a fornire una nuova piattaforma per la diffusione della disinformazione.

L'impatto della disinformazione può essere di vasta portata, con potenziali conseguenze per individui, organizzazioni e persino Paesi.

La disinformazione, come già anticipato, può essere usata per diffondere false voci, manipolare l'opinione pubblica e persino interferire con i processi democratici. Può anche portare all'erosione della fiducia nelle istituzioni e minare la coesione sociale.

Uno degli impatti più significativi della disinformazione è sulla salute pubblica.

[12] Clickbaiting: Adescamento a visitare le pagine di un sito Web, finalizzato all'aumento delle rendite pubblicitarie.

[13] Mass media: Insieme dei mezzi per diffondere e divulgare messaggi di diverso valore a un pubblico anonimo, indifferenziato e disperso; anche le tecniche con le quali gruppi specializzati elaborano e diffondono informazioni, messaggi, segni e simboli.

Durante la pandemia di SARS-CoV-2, la disinformazione sul virus[14] e sul suo trattamento è stata dilagante, generando confusione e sfiducia nella popolazione. Questo ha portato alla riluttanza di alcune persone a vaccinarsi o a seguire le linee guida della sanità pubblica, contribuendo alla continua diffusione del virus.

La disinformazione può anche essere usata per colpire gruppi o individui specifici, come politici o attivisti, con l'intento di screditarli o di minare il loro lavoro; nei casi più estremi, ciò può portare a molestie, minacce e persino a danni fisici.

La lotta alla disinformazione è una questione complessa che richiede un approccio multiforme. I governi, le organizzazioni della società civile e il settore privato hanno tutti un ruolo da svolgere nell'affrontare il problema.

Un approccio è quello di migliorare l'alfabetizzazione mediatica, che prevede l'educazione del pubblico su come identificare ed evitare la disinformazione. Ciò include l'insegnamento delle capacità di pensiero critico, delle tecniche di verifica dei fatti e la promozione dell'alfabetizzazione mediatica nelle scuole.

Un altro approccio consiste nel promuovere la trasparenza e la responsabilità online. Tale aspetto include la promozione di dati aperti e di un accesso aperto alle informazioni, nonché la promozione di pratiche etiche nel giornalismo e nei social media.

Le aziende di social media stanno prendendo sempre più provvedimenti per combattere la disinformazione sulle loro piattaforme. Hanno implementato politiche per rimuovere gli account falsi, limitare la diffusione di informazioni false ed etichettare i contenuti che sono stati sottoposti a fact-checking[15].

Tuttavia, si teme anche che questi sforzi possano essere insufficienti; alcuni critici sostengono infatti che le aziende di social media non stiano facendo abbastanza per rimuovere i contenuti dannosi o che i loro algoritmi possano in realtà amplificare la disinformazione promuovendo contenuti sensazionali o divisivi

I governi possono anche adottare misure per regolamentare le piattaforme online, comprese

[14] La diffusione del SARS-CoV-2 ha generato un'ondata di disinformazione. La circolazione di notizie false è stata favorita soprattutto dai social media, dai mass media, e dalle app di messaggistica. Nel 2022 è stato stimato che le Fake news sul SARS-CoV-2 generino un giro di affari di circa 1,1 miliardi di dollari annui, causando tuttavia danni agli individui e ai sistemi sanitari nazionali per cifre molto più elevate.

[15] Fact-checking: processo che cerca di verificare le informazioni fattuali, al fine di promuovere la veridicità e la correttezza di una notizia, prima che il testo sia diffuso, o dopo la sua diffusione. Fare fact-checking vuol dire effettuare una verifica puntigliosa dei fatti e delle fonti, tesa anche a valutare la fondatezza di notizie o affermazioni riguardanti istituzioni e persone di rilievo pubblico, con particolare riferimento a quanto viene diffuso mediante la Rete.

le società di social media, per garantire che si assumano la responsabilità dei contenuti che ospitano. Tali misure possono includere misure come l'etichettatura obbligatoria dei contenuti, la promozione del fact-checking e la regolamentazione della pubblicità politica.
La disinformazione online è un problema crescente che ha implicazioni significative per gli individui, le organizzazioni e persino i Paesi.
La lotta alla disinformazione richiede un approccio multiforme che comprende l'educazione del pubblico, la promozione della trasparenza e della responsabilità e la regolamentazione delle piattaforme online.
È essenziale agire per affrontare questo problema, per garantire che Internet rimanga una piattaforma di comunicazione libera e aperta e non uno strumento di manipolazione e inganno.

2.2 Deepfake

Come cita dogma.it: “Il deepfake è una tecnica utilizzata per la sintesi di immagini umane basata sull'intelligenza artificiale che utilizza la tecnologia di apprendimento automatico chiamata Generative Adversarial Networks per combinare e sovrapporre immagini e video esistenti con video o immagini originali. Il termine deepfake deriva dalla tecnologia sottostante "deep learning"[16], che è una forma di intelligenza artificiale”.

Il termine "deepfake" si riferisce a un tipo specifico di media sintetici, che in genere consiste nello scambiare il volto di una persona con il corpo di un'altra in un video o in un'immagine. La tecnologia alla base dei deepfake si basa su algoritmi avanzati di apprendimento automatico, come le reti generative avversarie (GAN), che sono in grado di creare immagini o video altamente realistici e convincenti. Addestrando questi algoritmi su grandi set di dati di immagini e video reali, i creatori di deepfake possono generare nuovi contenuti indistinguibili da quelli reali.

[16] Deep learning è un sottoinsieme del machine Learning (ML), in cui gli algoritmi di reti neurali artificiali sono modellati per funzionare come l'apparato cerebrale umano, imparando da grandi quantità di dati.

I deepfake possono essere utilizzati per un'ampia gamma di applicazioni lecite, dall'intrattenimento alla pubblicità; tuttavia, essi comportano anche rischi significativi per la società per l'intrinseco potenziale di inganno e disinformazione che presentano.

Uno degli usi più comuni della tecnologia deepfake è la creazione di contenuti di intrattenimento, come ad esempio video che presentano celebrità in scenari irrealistici o in ruoli che in realtà non hanno mai interpretato.
Sebbene questi tipi di deepfake siano generalmente innocui e possano essere divertenti, possono anche avere conseguenze indesiderate.
La tecnologia deepfake è progredita rapidamente negli ultimi anni, rendendo più facile per chiunque abbia un computer e una connessione a Internet creare video falsi convincenti.
I pericoli della tecnologia deepfake sono evidenti. Può essere usata per manipolare l'opinione pubblica, minare la fiducia nelle istituzioni democratiche e seminare discordia e confusione. Ad esempio, un video deepfake di una celebrità che dice o fa qualcosa di controverso potrebbe essere ampiamente condiviso sui social media, provocando un'indignazione pubblica e danneggiando potenzialmente la sua reputazione. Il potenziale di abuso è significativo ed è importante adottare misure per mitigare i rischi associati a questa tecnologia.
Uno dei modi più efficaci per combattere la tecnologia deepfake è l'educazione e la consapevolezza. È importante che le persone comprendano i pericoli dei deepfake e come possono essere identificati. Ciò può includere programmi di formazione per giornalisti, fact-checkers e altri professionisti che sono responsabili della verifica dell'autenticità dei contenuti.
Oltre alla formazione, esistono anche soluzioni tecniche che possono aiutare a combattere la tecnologia deepfake; tra queste, lo sviluppo di strumenti software in grado di rilevare video e immagini deepfake e l'uso della tecnologia blockchain per creare una registrazione a prova di manomissione dei contenuti digitali.
Un altro approccio alla lotta contro la tecnologia deepfake è l'utilizzo di quadri normativi e regolamentari. Ad esempio, alcuni Paesi hanno già emanato leggi che vietano la creazione e la distribuzione di contenuti deepfake senza il consenso delle persone che vi sono raffigurate.
Nonostante i potenziali pericoli associati alla tecnologia deepfake, è importante riconoscere

che questa tecnologia presenta anche molti potenziali vantaggi. Essa può essere utilizzata nell'industria dell'intrattenimento per creare effetti speciali realistici o nell'industria medica per creare simulazioni realistiche di procedure chirurgiche.

Un altro potenziale vantaggio della tecnologia deepfake riguarda la pubblicità e il marketing. Le aziende potrebbero utilizzare i deepfake per creare annunci altamente realistici con celebrità o modelli che non esistono realmente, il che potrebbe essere più conveniente rispetto all'assunzione di persone reali per il lavoro. Tuttavia, c'è il rischio che i consumatori vengano ingannati da questi annunci, in quanto potrebbero non rendersi conto che le persone che vi compaiono sono del tutto fittizie.

Come per ogni nuova tecnologia, la chiave è bilanciare i potenziali benefici con i potenziali rischi. Ciò richiede uno sforzo concertato da parte di governi, aziende tecnologiche e singoli individui per sviluppare soluzioni efficaci che possano contribuire a mitigare i rischi associati alla tecnologia deepfake.

La tecnologia deepfake è un campo in rapida evoluzione che ha il potenziale per rivoluzionare molti aspetti della nostra vita. Tuttavia, è importante adottare misure per mitigare i rischi associati a questa tecnologia. Ciò richiede una combinazione di educazione, soluzioni tecniche ed interventi legislativi e regolamentari che possano aiutare a garantire che questa tecnologia sia usata in modo responsabile ed etico.

2.2.1 Esempi di deepfake

L'esempio classico, e forse il più famoso, di deepfake è quello del video in cui l'ex presidente U.S.A. Barack Obama pronuncia un discorso in cui mette in guardia il mondo dai pericoli delle fake news e della disinformazione. Un discorso in realtà mai fatto da Obama: i creatori del video hanno infatti preso un video ufficiale dell'allora presidente degli Stati Uniti e vi hanno aggiunto un volto elaborato al computer, partendo dalle espressioni facciali dell'attore e regista americano Jordan Peele, che si è prestato all'esperimento. Questo è il caso più famoso di deepfake, che ha reso noto il fenomeno a livello globale, ma si tratta di un video risalente all'aprile 2018 mentre già dall'anno precedente si potevano reperire su Internet decine di video deepfake meno raffinati ma persino più inquietanti: i volti di attori e attrici famosi "montati" in scene di film pornografici, con un effetto assolutamente realistico.

Più goliardici, ma non meno raffinati, i video in cui il volto dell'attore Nicolas Cage veniva inserito in scene di film che non ha mai girato: da Indiana Jones a 007.

2.3 La manipolazione delle immagini online

La manipolazione di immagini online, o manipolazione di immagini digitali, è il processo di alterazione o modifica di immagini digitali mediante l'uso di software per computer. Essa è diventata sempre più popolare negli ultimi anni. Con l'avvento dei social media e la disponibilità diffusa di software di fotoritocco, le persone sono ora in grado di manipolare facilmente le immagini per adattarle alle proprie esigenze. Se da un lato questo può essere uno strumento utile per artisti e designer, dall'altro può essere utilizzato in modo ingannevole o dannoso.

La manipolazione delle immagini online può essere utilizzata per una serie di scopi, sia positivi che negativi.

Uno dei vantaggi più evidenti della manipolazione delle immagini online è che permette di creare immagini più accattivanti. Ad esempio, si può utilizzare un software di fotoritocco per ravvivare un'immagine spenta o per aggiungere filtri che le conferiscano un aspetto più interessante. Questo può essere particolarmente utile per le aziende o i privati che vogliono promuoversi online, in quanto possono utilizzare le immagini “ritoccate” per creare un aspetto più professionale e curato.

Un altro vantaggio della manipolazione delle immagini online è che può essere utilizzata per creare arte. Molti artisti utilizzano il software di fotoritocco per creare immagini surreali o astratte che sarebbero difficili o impossibili da realizzare nella vita reale. Questo può essere un ottimo modo per esprimere la propria creatività ed esplorare nuove tecniche artistiche.

Sul versante negativo, la manipolazione digitale delle immagini può essere utilizzata per ingannare o fuorviare le persone.

Le immagini online possono essere manipolate per cambiarne il significato o il contesto o per creare un falso senso della realtà. Ad esempio, essa può essere utilizzata per creare notizie false, alterare immagini politiche per trasmettere un determinato messaggio o creare prove false in casi legali.

Una delle forme più comuni di manipolazione digitale delle immagini è il fotoritocco.

I software di fotoritocco, come Adobe Photoshop, consentono agli utenti di manipolare le immagini in vari modi. Gli utenti possono ritagliare le immagini, regolare il bilanciamento del colore, aggiungere testo e applicare effetti speciali.

Il fotoritocco può essere utilizzato per migliorare la qualità visiva delle immagini, ma anche per manipolarle in modo ingannevole. Inoltre, un'altra forma di manipolazione digitale delle immagini è il deepfake, di cui abbiamo parlato al paragrafo 2.2.

La manipolazione dell'immagine online può anche contribuire a creare problemi di immagine corporea e standard di bellezza irrealistici. Quando le persone vedono immagini pesantemente modificate di modelli o celebrità, possono iniziare a pensare di dover apparire in un certo modo per essere attraenti o avere successo.

La manipolazione delle immagini online può avere gravi conseguenze. Ad esempio, le notizie false create con immagini manipolate possono influenzare l'opinione pubblica e causare danni. Le immagini politiche manipolate per trasmettere un determinato messaggio possono influenzare l'opinione pubblica e il risultato delle elezioni.

I deepfake creati per ingannare le persone possono causare gravi danni agli individui e alla società nel suo complesso.

Per combattere gli effetti negativi della manipolazione delle immagini digitali, è importante educare le persone a riconoscere le immagini manipolate. Ci sono diversi segnali che indicano che un'immagine è stata manipolata, come l'illuminazione non corrispondente, le ombre non realistiche e le proporzioni distorte. È inoltre importante sviluppare una tecnologia in grado di rilevare i deepfake e altre forme di manipolazione delle immagini digitali.

Per concludere, la manipolazione delle immagini online può essere utilizzata sia per scopi positivi che negativi.

Se da un lato essa può essere utilizzata per migliorare la qualità visiva delle immagini, dall'altro può essere usata per ingannare o fuorviare le persone. Per combattere gli effetti negativi della manipolazione delle immagini digitali, è quindi importante, come detto, educare le persone a identificare le immagini manipolate e sviluppare una tecnologia in grado di rilevare i deepfake e altre forme di manipolazione delle immagini digitali.

2.4 Modifica di post sui social media

L'alterazione dei contenuti online è diventata un problema sempre più diffuso nell'odierna era digitale. Una forma di alterazione dei contenuti online che ha suscitato grande attenzione è la modifica dei post sui social media. Le piattaforme dei social media sono diventate un mezzo primario di comunicazione e condivisione delle informazioni per molti individui e organizzazioni, il che le rende un obiettivo prezioso per chi cerca di manipolare o diffondere informazioni false. La modifica dei post sui social media può avere un impatto significativo sulla diffusione delle informazioni e può essere utilizzata sia per scopi illeciti che legittimi.

La modifica di un post sui social media comporta l'apporto di modifiche al testo, all'immagine o al contenuto video originale dopo la sua pubblicazione. Ciò può includere la correzione di errori, l'aggiornamento di informazioni o la modifica del significato del post originale. Sebbene la modifica dei post possa sembrare un'azione semplice e innocua, può avere implicazioni di vasta portata per l'autenticità e la credibilità dei contenuti online.

Una delle implicazioni più preoccupanti è il potenziale di disinformazione che tale attività presenta.

La modifica di un post per cambiarne il significato o lo scopo può essere usata per ingannare e manipolare il pubblico; ad esempio, un politico potrebbe modificare un tweet per cambiare la propria posizione su una questione critica, ingannando i propri follower e cambiando la percezione pubblica delle proprie convinzioni. Allo stesso modo, un individuo o un'organizzazione potrebbe modificare un post per affermare falsamente che un prodotto o un servizio ha ricevuto recensioni o riscontri positivi.

Inoltre, la modifica dei post sui social media può avere conseguenze negative sulla credibilità e sull'autenticità dei contenuti online.

Poiché le piattaforme dei social media sono diventate una fonte primaria di informazioni e notizie, i post modificati possono compromettere l'affidabilità delle fonti di informazione online. La facilità di modifica dei post e la mancanza di responsabilità per le alterazioni rendono difficile distinguere tra informazioni legittime e false o modificate.

Tuttavia, la modifica dei post sui social media può anche avere scopi legittimi, come la correzione di errori di fatto o l'aggiornamento delle informazioni. Ciò può essere particolarmente rilevante in situazioni in cui il post originale conteneva informazioni imprecise o fuorvianti. Ad esempio, un giornalista potrebbe modificare un tweet per

correggere un errore di fatto in una notizia dell'ultim'ora, assicurando così la diffusione di informazioni accurate al pubblico.

Riassumendo, la modifica dei post sui social media può avere implicazioni significative per la diffusione delle informazioni e l'autenticità dei contenuti online.

Se da un lato può essere utilizzato per scopi legittimi, come la correzione di errori o l'aggiornamento di informazioni, dall'altro può essere usato per ingannare e manipolare il pubblico.

Pertanto, anche in questo ambito, è essenziale essere vigili e valutare criticamente l'autenticità dei contenuti online, in particolare sulle piattaforme dei social media. Inoltre, le piattaforme di social media e le organizzazioni dovrebbero implementare misure per impedire la modifica dei post che contengono disinformazione e informazioni errate. In questo modo, possiamo garantire la credibilità e l'autenticità dei contenuti online, promuovendo così un processo decisionale informato e un ecosistema digitale sano.

2.5 Creazione di siti web falsi

Come già diffusamente argomentato, Internet è diventato una parte essenziale della nostra vita quotidiana e vi facciamo affidamento per vari scopi, come la comunicazione, l'informazione e le transazioni online. Tuttavia, con l'avvento di Internet, anche la criminalità informatica si è evoluta di pari passo, e una delle sue minacce più significative è la creazione di siti web falsi. I siti web falsi sono progettati per assomigliare a quelli legittimi, ma sono hanno lo scopo di ingannare gli utenti e rubare le loro informazioni personali e finanziarie.

La creazione di un sito web falso è un processo che prevede la progettazione e la pubblicazione di un sito web che sembra autentico ma che ha lo scopo di ingannare i visitatori e comporta rischi significativi per gli utenti.

I criminali informatici creano questi siti web con l'obiettivo di attirare gli utenti ignari e indurli a fornire le loro informazioni personali e finanziarie, come i dati della carta di credito, le password bancarie ed altri dati sensibili. I criminali utilizzano poi queste informazioni per furti di identità, frodi e altre attività illegali.

Il primo passo per creare un sito web falso è identificare il pubblico di riferimento.

Il sito web deve essere progettato in modo da soddisfare gli interessi e le esigenze delle

vittime previste ed attirare la loro attenzione.
Ad esempio, se l'obiettivo è un cliente di una banca, il sito web falso può imitare la pagina di login della banca o il portale di online banking; se l'obiettivo è un utente di social media, il sito Web falso può imitare la pagina di accesso della piattaforma di social media.
Una volta identificato il pubblico target, il passo successivo è la progettazione del sito web. Questo deve avere un aspetto professionale e legittimo, utilizzando loghi, immagini ed elementi di design simili a quelli del sito web reale.
Il sito web può utilizzare un nome di dominio o un URL simile, con solo piccole variazioni, come l'uso di un trattino o l'errore di battitura di una parola.
Il falso sito web contiene in genere informazioni convincenti e autorevoli, come testimonianze, recensioni di clienti o articoli di cronaca; può anche includere certificati di sicurezza falsi, come i loghi SSL o Verisign, per dare l'impressione di legittimità.
Il linguaggio e il tono del sito web appaiono persuasivi e convincenti, utilizzando tattiche psicologiche per incoraggiare i visitatori ad interagire inducendoli a fornire i propri dati sensibili.
I siti web falsi possono utilizzare varie tecniche, come il phishing, lo spoofing e il domain hacking.
Il phishing consiste nell'invio di e-mail fraudolente che sembrano provenire da una fonte legittima, come una banca, un social media o un sito di e-commerce, per indurre gli utenti a fornire le proprie credenziali di accesso e informazioni personali.
Lo spoofing consiste nel creare un sito web che sembra legittimo, ad esempio un sito di shopping online, per indurre gli utenti a effettuare acquisti e a fornire le proprie informazioni finanziarie.
Il domain hacking consiste nel rubare il nome di dominio di un sito web legittimo e reindirizzare gli utenti a un sito web falso.
Un altro uso dei siti web falsi è la distribuzione di malware.
Il malware è un software progettato per danneggiare o disabilitare i sistemi informatici o per rubare informazioni sensibili. I criminali possono creare siti web falsi che contengono malware, come virus o trojan, che vengono poi scaricati sul computer della vittima. Il sito Web falso appare in tutto e per tutto come legittimo, assumendo le medesime caratteristiche, ad esempio, di un sito di download di software o di file-sharing.

L'impatto dei siti web falsi sugli utenti può essere devastante, con perdite finanziarie, furti di identità e punteggi di credito danneggiati. Inoltre, i siti web falsi possono danneggiare la reputazione delle organizzazioni legittime che vengono impersonate dai criminali. La creazione di siti web falsi può anche ridurre la fiducia degli utenti nel commercio elettronico e in altre transazioni online, limitando la crescita e lo sviluppo dell'economia digitale.
Per combattere la creazione di siti web falsi, gli utenti devono essere vigili e cauti quando forniscono informazioni personali e finanziarie online.
È importante verificare l'autenticità dei siti web prima di fornire informazioni sensibili, ad esempio controllando l'URL, cercando il simbolo del lucchetto e confermando il certificato SSL.
Inoltre, i gestori (internet provider) possono implementare misure come l'autenticazione a più fattori, il rilevamento delle frodi e la crittografia per proteggere le informazioni degli utenti dai criminali informatici.
Per concludere, la creazione di siti web falsi è una minaccia significativa per la sicurezza online e comporta gravi rischi per gli utenti.
La facilità nel creare siti web falsi e la crescente sofisticazione dei criminali informatici rendono essenziale che gli utenti siano vigili e cauti nel fornire informazioni sensibili online, così come anche i fornitori dei servizi Internet devono implementare solide misure di sicurezza per proteggere i propri utenti dalla criminalità informatica e garantire l'integrità e la credibilità dei propri contenuti online.

2.6 Spamming di recensioni online

L'aumento dell'e-commerce e delle aziende online ha portato a un incremento dell'importanza delle recensioni online.
Le recensioni online svolgono un ruolo cruciale nella formazione della reputazione di un'azienda.
Nel mondo digitale di oggi, i potenziali clienti si rivolgono alle recensioni online per valutare la qualità di prodotti e servizi prima di effettuare un acquisto; di conseguenza, le aziende si sforzano di mantenere recensioni e valutazioni positive per attirare e fidelizzare i clienti. Tuttavia, alcune aziende ricorrono a pratiche non etiche, come lo spam delle recensioni online, per migliorare le proprie valutazioni.

Lo spamming di recensioni online si riferisce alla pratica di pubblicare recensioni false o fuorvianti per migliorare il rating di un'azienda.

Alcune aziende si rivolgono a servizi terzi specializzati nella generazione di recensioni positive in gran numero. Queste recensioni sono solitamente scritte da recensori appositamente ingaggiati e retribuiti che non hanno alcuna esperienza con il prodotto o il servizio che stanno recensendo, e sono quindi sostanzialmente false. Alcune aziende incentivano i clienti a pubblicare recensioni positive offrendo sconti o prodotti gratuiti. In alcuni casi, anche i concorrenti possono “spammare” recensioni negative per danneggiare la reputazione di un'azienda.

L'impatto dello spam di recensioni online può essere dannoso per le aziende e per i consumatori.

I clienti si affidano sempre più frequentemente alle recensioni per prendere decisioni informate su prodotti e servizi. Le recensioni false possono quindi indurre i clienti ad acquistare prodotti o servizi di bassa qualità che non soddisfano le loro aspettative. Questo può portare all'insoddisfazione dei clienti, a riscontri negativi e, in ultima analisi, alla perdita di affari per le aziende interessate. Inoltre, lo spam di recensioni online può creare un vantaggio sleale per le aziende che si dedicano a questa pratica non etica, avvantaggiandole rispetto a quelle oneste che si affidano ai feedback autentici dei clienti.

Piattaforme online come Google, Yelp e Amazon sono consapevoli del problema dello spam delle recensioni online e hanno implementato le misure per combatterlo.

Queste piattaforme utilizzano algoritmi che individuano e filtrano le recensioni false. Inoltre, incoraggiano i clienti a segnalare le recensioni sospette, che vengono poi esaminate dai moderatori dei contenuti della piattaforma.

In alcuni casi, le piattaforme possono anche intraprendere azioni legali contro le aziende che si dedicano allo spam di recensioni online.

Per quanto concerne l’atteggiamento delle aziende, che offrono i propri prodotti e servizi ad un’ampia platea di consumatori, è essenziale mantenere l'onestà e l'integrità quando si tratta di recensioni online; ciò include l'astenersi dall'incentivare i clienti a pubblicare recensioni positive e l'evitare l'uso di recensioni false per migliorare le valutazioni.

Le aziende devono invece concentrarsi sulla fornitura di prodotti e servizi di qualità, che genereranno naturalmente e spontaneamente recensioni positive da parte dei clienti

soddisfatti. Dovrebbero inoltre incoraggiare i clienti a lasciare recensioni oneste e rispondere alle recensioni negative in modo costruttivo.

Lo spam di recensioni online è una pratica non etica che danneggia le aziende e i consumatori.

Infatti, le recensioni false ingannano i clienti e creano un vantaggio sleale per le aziende che si dedicano a questa pratica. Le piattaforme online dispongono di misure per combattere lo spamming di recensioni online, ma anche le aziende hanno la responsabilità di mantenere l'integrità e l'onestà quando si tratta di recensioni online. Fornendo prodotti e servizi di qualità ed incoraggiando il feedback corretto dei clienti, le aziende possono mantenere una reputazione positiva e fidelizzare la loro clientela.

2.7 Manipolazione dei motori di ricerca

La manipolazione dei motori di ricerca è una forma di alterazione dei contenuti online che comporta la pratica di aumentare artificialmente la visibilità e il posizionamento di specifici siti web o contenuti nelle pagine dei risultati dei motori di ricerca (SERP).

L'obiettivo di tale attività consiste nel manipolare gli algoritmi dei motori di ricerca per favorire specifici siti web, marchi o individui rispetto ad altri, e le implicazioni di questa pratica possono essere significative.

La manipolazione dei motori di ricerca può assumere varie forme, tra cui il keyword stuffing, il cloaking, le link farm e il testo nascosto.

Il keyword stuffing consiste nel riempire i contenuti con parole chiave irrilevanti o ripetitive per posizionarsi più in alto nei risultati dei motori di ricerca.

Il cloaking consiste nel mostrare ai motori di ricerca contenuti diversi da quelli visibili all'utente, in modo da ottenere un posizionamento più elevato nei risultati dei motori di ricerca.

Le link farm sono siti web creati al solo scopo di fornire link ad altri siti web; questi link sono spesso di bassa qualità e irrilevanti per il contenuto del sito.

Il testo nascosto consiste invece nell'utilizzare un testo dello stesso colore dello sfondo di un sito web, nel tentativo di nasconderlo agli utenti ma di renderlo visibile ai motori di ricerca.

Queste tecniche sono considerate non etiche e possono comportare la penalizzazione di un sito web o addirittura il divieto di accesso ai motori di ricerca.

L'impatto della manipolazione dei motori di ricerca può essere significativo e portare a pubblicità ingannevole, riduzione della fiducia degli utenti nei motori di ricerca e concorrenza sleale.
La manipolazione dei risultati dei motori di ricerca può indurre gli utenti a credere che un sito web o un contenuto sia più rilevante o credibile di quanto non sia, con conseguente pubblicità ingannevole e spreco di risorse.
Inoltre, la manipolazione dei motori di ricerca può danneggiare la reputazione di siti web e aziende che operano correttamente, con conseguente riduzione del loro potenziale economico e di vendita.
Per combattere la pratica della manipolazione dei motori di ricerca, quest'ultimi devono implementare misure per individuare e penalizzare le pratiche di manipolazione.
Ciò può essere realizzato analizzando i contenuti dei siti web, rilevando modelli di link sospetti e valutando il comportamento degli utenti per identificare le pratiche di manipolazione. Inoltre, i motori di ricerca possono fornire trasparenza sui loro algoritmi di ranking, educare gli utenti sulle pratiche di manipolazione e incoraggiare le pratiche SEO legittime che danno priorità ai contenuti di qualità e all'esperienza dell'utente.
Possiamo quindi affermare che la manipolazione dei motori di ricerca è una minaccia significativa per l'integrità dei contenuti online e può avere implicazioni significative sia per gli utenti che per le aziende.
E' pertanto essenziale implementare misure per individuare e penalizzare le pratiche di manipolazione e promuovere pratiche SEO legittime che diano priorità ai contenuti di qualità e all'esperienza dell'utente, al fine di promuovere la trasparenza e l'integrità dei contenuti online e garantire condizioni di parità per le aziende e gli individui.

2.8 Cybercrime, la terza economia mondiale

Nella società odierna sono sempre più frequenti le frodi perpetrate tramite mezzi telematici. Quasi un italiano su tre (il 27,2%), è stato vittima di una truffa informatica. Il 15,3% ha subìto un raggiro dovuto a una falsa identità e il 13,2% è stato oggetto di furto d'identità. Tutte le tecniche utilizzate hanno come comune denominatore lo sfruttamento della fiducia

dell'utente per carpire o manipolare dati, rubare denaro, eludere i controlli di accesso alle reti e diffondere malware tramite link e allegati malevoli.

Secondo il Rapporto Annuale sulle Minacce Informatiche di Thales, in Italia il numero di attacchi è in netto aumento. Si consideri inoltre che qualunque conteggio in tale ambito deve necessariamente ritenersi approssimato per difetto, poiché tanti attacchi o truffe informatiche non vengono denunciate per riluttanza dei soggetti raggirati e, talvolta, perché essi provano vergogna nell'ammettere di essere stati ingannati. Inoltre, sempre dal Rapporto pubblicato da Thales, emerge non solo che il numero di cyberattacchi in Italia sta aumentando, ma anche che più della metà delle aziende (51%) non ha un piano per proteggersi. Quasi la metà dei professionisti intervistati segnala un aumento degli attacchi ransomware, virus che bloccano un sistema informatico e/o un data base che viene sbloccato solo dietro il pagamento un riscatto. Per questo motivo il direttore Frattasi, nominato di recente alla guida dell'Agenzia per la cybersicurezza nazionale, ha ricordato quanto la sicurezza informatica sia un problema che coinvolge tutti i cittadini perché grande è il rischio che i dati personali possano essere diffusi oppure che vengano bloccati servizi essenziali, sanità o trasporti, come dimostrano gli attacchi al sistema vaccinale del Lazio e ad alcuni operatori della mobilità pubblica, come Atm e Atac.

"Si stima che il mondo del cybercrime sia la terza economia mondiale, subito dopo Stati Uniti e Cina", ha dichiarato Tommaso Profeta, Managing Director della Divisione Cyber & Security Solutions di Leonardo.

È quindi evidente l'esigenza di dotarsi di figure professionali capaci di fronteggiare la minaccia, ma ad oggi sono 3,4 milioni gli specialisti che mancano nel mondo per colmare questo divario. Questi numeri testimoniano la necessità di puntare in modo deciso sulla formazione di giovani esperti e in generale di aumentare la consapevolezza dei pericoli, tanto che l'85% degli attacchi vanno a buon fine a causa di errori umani. Per cercare di colmare questa necessità è stata istituita da Leonardo la Cyber & Security Academy, una scuola di alta formazione sia per istruire nuovi operatori tecnici del settore che per aumentare la sensibilizzazione nel personale non specializzato ma con ruoli chiave all'interno di aziende o Pubblica Amministrazione.

CAPITOLO 3

CONSEGUENZE ECONOMICHE E LEGALI

3.1 Impatto economico dell’alterazione dei contenuti online

L'alterazione dei contenuti online ha un impatto economico significativo sia a livello globale che individuale.

Questo fenomeno riguarda la manipolazione di informazioni o la creazione di notizie false o fuorvianti su internet, che può danneggiare l'economia, le imprese e le persone che dipendono dalle informazioni accurate per prendere decisioni.

Le conseguenze dell'alterazione dei contenuti online si ripercuotono in diversi settori dell'economia. In primo luogo, le aziende possono subire danni economici a causa di notizie false o fuorvianti che influenzano le decisioni degli investitori o dei consumatori. Ad esempio, se una società viene accusata di comportamenti illeciti sulla base di informazioni false, le sue azioni possono subire una caduta improvvisa e causare gravi danni finanziari. Inoltre, i consumatori possono subire danni economici se acquistano prodotti basati su recensioni false o manipolate.

L'alterazione dei contenuti online può anche influenzare l'economia globale. Ad esempio, la diffusione di notizie false può influenzare i mercati finanziari e provocare fluttuazioni estreme.

Esemplificativo in tal senso è quanto recentemente avvenuto (23 maggio 2023) allorquando la sola pubblicazione su Twitter di una falsa fotografia generata dall’Intelligenza Artificiale e raffigurante un’esplosione nei pressi del Pentagono, sede del Dipartimento della Difesa degli Stati Uniti, ha immediatamente causato una perdita di 30 punti in pochi minuti dell’indice S&P 500 della Borsa di Wall Street.

Appare a tutti evidente, in un’epoca come la nostra in cui le reazioni economico - finanziarie ad un evento percepito come dannoso o pregiudizievole sono pressoché immediate, come l’alterazione di un contenuto online, ovvero la diffusione di contenuti falsi, siano attività ampiamente idonee a causare rilevanti effetti negativi.

Sotto un ulteriore aspetto, anche le campagne pubblicitarie basate su informazioni false o manipolate possono influenzare le decisioni degli investitori e le scelte dei consumatori, compromettendo la fiducia nel mercato.

Inoltre, si può danneggiare la reputazione delle imprese e dei singoli individui. Le notizie false possono diffamare un'azienda o una persona, influenzando la percezione che il pubblico ha di essa. Questo può portare a perdite di clienti, opportunità di lavoro e potenziali entrate.

In rete circolano ormai milioni di notizie false che creano nuovi rischi per la reputazione di imprese e persone. La spinta ad accelerare questo fenomeno è in gran parte dovuta alla proliferazione di Internet e dei social network. Chi pensa che questo fenomeno riguardi solo determinate zone si sbaglia. Dalle notizie alla salute alla finanza, le notizie false hanno permeato quasi tutti i settori. Il settore aziendale non fa eccezione, con un crescente bisogno di firme per la gestione del rischio reputazionale[17].

I contenuti di notizie false generalmente imitano il formato e il tono delle notizie reali, ma non sono sottoposti al processo di verifica oggettiva che è alla base del giornalismo.

Le aziende stanno iniziando a rispondere, ma la discriminazione temporale continua a svolgere un ruolo importante.

Fermare la diffusione e la velocità di replicazione delle fake news con informazioni corrette non è un'impresa facile. Che si tratti di iniziative individuali spesso dominate da ideologie antiindustriali o di attacchi mirati da parte di attori che cercano di causare danni economici, gli obiettivi dei detrattori sono sempre comuni: diffamare e minare la fiducia tra consumatori e imprese.

I rischi reputazionali sono influenzati principalmente da tre fattori, i quali hanno contribuito alla diffusione della disinformazione online.

Il primo fattore è il tempo. Nel mondo digitale, il contenuto è permanente; l'accesso alle informazioni si basa sulla pertinenza, non sulla novità. Il tempo non è continuo come nel mondo della carta stampata, dove le informazioni vengono diffuse attraverso i media tradizionali che hanno un alto grado di accessibilità per giorni e un rapido decadimento (decadimento dei contenuti) nel tempo, ma tutto diventa un continuum che esiste contemporaneamente. Grazie ai motori di ricerca, i contenuti web rimangono accessibili per molto tempo.

Il secondo fattore è l'autorevolezza. Sulla carta stampata la firma di un giornalista ha un valore chiaro e riconosciuto; al contrario, il mondo digitale guarda con sospetto alle fonti

[17] Il rischio reputazionale è il rischio attuale o prospettico di flessione degli utili o del capitale derivante da una percezione negativa dell'immagine dell'azienda da parte di clienti, controparti, azionisti, investitori o autorità di vigilanza (definizione di Banca d'Italia).

istituzionali e le considera non oggettive.

Il terzo fattore è il controllo. Prima del mondo online, la comunicazione era un flusso dall'alto verso il basso. I brand parlavano e gli utenti potevano solo ascoltare o cambiare canale. Ciò ha consentito un maggiore controllo sulla diffusione delle informazioni e sulla conseguente reputazione. In un mondo digitale chiunque può scrivere, tutti possono essere editori e la comunicazione sarà non mediata e orizzontale. Oggigiorno i brand non sono più la fonte primaria di informazioni. La perdita di controllo è dovuta a due fattori: la velocità e la viralità.

Possiamo pertanto affermare che l'alterazione dei contenuti online ha un impatto economico significativo su molteplici livelli, dalle aziende ai consumatori e all'economia globale.

È quindi importante che governi, aziende e individui collaborino per combattere questo fenomeno e preservare la fiducia nel mercato e nella società.

La diffusione di notizie accurate e di alta affidabilità è essenziale per la stabilità e la prosperità dell'economia e della società nel loro complesso.

3.2 Conseguenze legali per i reati dell'alterazione dei contenuti online

L'argomento delle conseguenze legali per i reati di alterazione online è molto delicato e ampio.

Creare un profilo falso è legale, ma farlo utilizzando l'identità di un'altra persona costituisce reato di furto d'identità o frode. Insulto o diffamazione nella realtà o online sono entrambi illeciti, ma farlo in rete è più grave in quanto quel messaggio può rimanere per molto tempo e raggiungere un pubblico più ampio. Questa dimensione è più pervasiva.

Ci sono casi in cui il diritto non ha strumenti per punire alcune situazioni online, che però vengono punite nella realtà.

Ad esempio, la diffusione di informazioni false in rete non è coperta da nessuna norma perché una sorta di "disinformazione" nella realtà è stata sempre accettata, in quanto può considerarsi indirettamente tutelata dall'articolo 21 della Costituzione sulla libertà d'espressione.[18]

[18] Art. 21: Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure.

La rete, con la sua capacità espansiva, favorisce una diffusione maggiore di questo tipo di informazioni perché alimentata da una quantità enorme di soggetti. Tempo e spazio sono molto più ristretti; per questo il diritto non riesce ad anticipare le possibili condotte illecite ed è sempre in ritardo.

Nella dimensione online il limite dell'espressione è difficile da tracciare, dato che ci troviamo in un contesto policentrico. Il limite posto dal nostro ordinamento stabilisce che si devono tutelare onore e reputazione della persona.

Il tema del rapporto tra diritto, internet ed il suddetto limite è di difficile lettura per l'estrema mobilità delle notizie sulla rete.

Il diritto non ha agito allo stesso modo sui temi della responsabilità online e offline: in quest'ultimo caso, viene punito che è responsabile di aver commesso il fatto; nel primo, viene punito chi gestisce le piattaforme online (ISP, Internet Service Provider) su cui i contenuti sono condivisi.

Può apparire quasi inutile punire chi commette un illecito online, perché in un ristrettissimo lasso temporale ne vengono commessi migliaia ed a volte è impossibile risalire con certezza all'individuo che lo ha commesso.

È un tema molto controverso perché, intervenendo con decisione ed incisività a livello legislativo, si rischierebbe di autorizzare, in qualche modo, una sorta di Stato di polizia che censura i diritti fondamentali dei cittadini.

In altre parole, si aumenterebbe il potere punitivo di uno Stato, in evidente contrasto con il concetto di diritto come strumento per prevenire piuttosto che per sanzionare.

D'altro canto, considerato che la dimensione online ha più rischi di quella offline, e al contempo più possibilità, questa eccessiva libertà può portare ad una maggiore discriminazione verso i soggetti più "deboli".

Allo stato attuale, l'indicazione giuridica prevalente è di non sanzionare tanto chi commette il fatto, quanto chi offre il servizio sul quale il fatto stesso viene commesso.

La grande differenza tra gli ISP[19] è tra gli hosting (Youtube, Instagram, Facebook) e content (siti d'informazione, blog) provider.

---

[19] ISP, Internet Service Provider, nelle telecomunicazioni, indica un'organizzazione o un'infrastruttura che offre agli utenti (residenziali o imprese), dietro la stipulazione di un contratto di fornitura, servizi inerenti a Internet, i principali dei quali sono l'accesso al World Wide Web e la posta elettronica". Fonte: Treccani.

Nei primi la piattaforma è il tramite per la fruizione del servizio, nei secondi fornisce un suo proprio servizio.

Google, con la sua indicizzazione (scegliendo il posizionamento dei risultati della ricerca), è considerato sia hosting che content provider; in questo caso si può anche parlare di sharing provider: fornitore di un servizio per la condivisione dei contenuti.

Di norma, l'hosting provider è considerato non responsabile dell'illecito, a meno che non ne sia venuto a conoscenza. Per quanto riguarda la pubblicazione di una foto di una persona su un hosting provider, il limite è rappresentato dal rispetto della dignità e reputazione del soggetto raffigurato.

La questione è alquanto delicata e ruota intorno alla circostanza per cui un ISP debba - e possa - decidere cosa è illecito o no; quindi, se un soggetto privato possa ergersi a colui che applica il diritto, ovvero se una piattaforma debba rimanere indifferente di fronte a questo tipo di condotte illecite.

Fino a che punto i social sono tenuti a rimuovere i contenuti sulle proprie piattaforme?

Il loro compito è quello di informare l'autorità pubblica dell'illecito riscontrato; hanno cioè un ruolo di collaborazione.

Gli ISP non sono responsabili dei contenuti in essi presenti, in quanto non hanno obblighi di sorveglianza. La loro diretta responsabilità è ravvisabile solo in tre casi:

1. Quando sono loro a immettere il contenuto (quando compiono una condotta tale per cui l'illecito è a loro imputabile); ci si riferisce ai content provider e agli hosting attivi (coloro che compiono un'attività che fa sì che un determinato contenuto veda la partecipazione attiva del provider; es. indicizzazione praticata da Google);
2. Quando c'è un ordine dell'autorità pubblica (giudiziaria o amministrativa) e loro non lo osservano;
3. Quando non collaborano con le autorità di pubblica sicurezza nonostante venga loro segnalata una condotta illecita.

Questa normativa, stabilita dalla direttiva comunitaria 2000/43/CE[20], è stata applicata negli anni dalla giurisprudenza europea.

Con la sua impostazione tendenzialmente liberale, è volta, da una parte, a preservare i diritti

[20] Il 29 giugno 2000 il Consiglio ha adottato la direttiva 2000/43/CE (6) che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica, la quale assicura una protezione contro tali discriminazioni nel settore dell'occupazione e delle condizioni di lavoro.

economici del social, senza richiedere loro un'attività sproporzionata; dall'altro è volta a preservare il ruolo dell'autorità pubblica.

A partire dal 2014-2015, l'orientamento cambia: con lo scandalo di Wikileaks e con la sentenza di Google Spain sul diritto all'oblio, si comincia a richiedere e pretendere una maggiore responsabilità da parte degli ISP.

In quegli anni, ci sono una serie di sentenze volte a rafforzare la responsabilità dei social e ad aumentare il controllo su di essi.

La Corte di Giustizia afferma che i social, quando vengono a conoscenza di un illecito, devono attivarsi affinché che quell'illecito non venga ripetuto, introducendo tacitamente un obbligo di sorveglianza; il social ha quindi l'obbligo, e non la mera facoltà, di rimuovere i contenuti illeciti.

Considerando le rilevanti responsabilità in discussione, si è ritenuto opportuno che i social cooperassero con le autorità competenti nello stabilire delle regole di comportamento. Nascono così nel 2018 dei codici di condotta per contrastare gli hate speeches e le fake news: entro 48 ore dalla segnalazione di un illecito, il contenuto deve essere valutato dal social, ed entro ulteriori 48 ore rimosso, se del caso.

Il risultato è che gran parte dell'attività di rimozione di contenuti illeciti dai social è svolta dai provider stessi, con maggiore rapidità d'intervento.

Rebus sic stantibus, è evidente l'insorgere del tema relativo alla democraticità dei gestori dei social: finché questi applicano criteri improntati alla democraticità del loro operato, non c'è rischio per gli utenti di vedersi negato o ingiustamente limitato l'esercizio dei loro diritti.

La giurisprudenza italiana sul tema della responsabilità degli ISP è stata finora piuttosto ambigua e, nel corso degli anni, vi sono state sentenze di condanna nei confronti degli ISP piuttosto controverse.

Si pensi al caso in cui il social network Facebook venne condannato in quanto il video intimo pubblicato ad insaputa della povera Tiziana Cantone era ancora disponibile sulla piattaforma, e non era stato rimosso nonostante il tragico esito della vicenda.

Nel 2019, dopo la sentenza di appello, la Cassazione affermò che un ISP è responsabile quando non può non conoscere il carattere illecito del contenuto caricato all'interno della propria piattaforma (sia esso segnalato da un utente, dai giornali o da altra fonte) e non si adopera tempestivamente per rimuoverlo.

Sotto ulteriore aspetto, appare opportuno soffermarsi anche sui reati di alterazione dei contenuti online, che si concretizzano in atti con cui un individuo modifica, cancella o aggiunge contenuti su un sito web o su qualsiasi piattaforma online senza autorizzazione. Queste azioni possono avere conseguenze legali significative, tra cui alcune di rilevanza penale, nonché di responsabilità civile per danni alla reputazione.

Negli U.S.A., nazione ritenuta particolarmente sensibile a questi temi ed all'avanguardia nel legiferare in materia, alcune delle accuse penali più comuni per i reati di alterazione di contenuti online includono:

1. Computer Fraud and Abuse Act (CFAA): la CFAA è una legge federale che vieta agli individui di accedere a computer o sistemi informatici protetti senza autorizzazione o di superare l'accesso autorizzato. Questa legge punisce anche qualsiasi atto di distruzione, modifica o interruzione dei servizi informatici. Le violazioni della CFAA possono comportare pene severe, tra cui la reclusione ed ingenti multe.
2. Electronic Communications Privacy Act (ECPA): l'ECPA è una legge federale che proibisce l'intercettazione e la divulgazione delle comunicazioni elettroniche, comprese le e-mail e i messaggi istantanei. Questa legge punisce anche l'accesso non autorizzato alle comunicazioni elettroniche memorizzate; le violazioni dell'ECPA possono comportare pene detentive e pecuniarie.
3. Legge sul furto d'identità: questa legge federale criminalizza il furto dell'identità di un'altra persona per commettere reati di alterazione di contenuti online. Le violazioni di questa legge possono comportare la reclusione ed ingenti multe.
4. Leggi statali sui crimini informatici: molti Stati U.S.A. hanno emanato proprie leggi per criminalizzare i reati di alterazione di contenuti online. Queste leggi spesso rispecchiano le leggi federali di cui sopra e possono comportare sanzioni simili.

Alcune delle tipologie più comuni di cause civili connesse all'alterazione o diffusione di contenuti online sono:

1. Diffamazione: la diffamazione si verifica quando una persona svolge affermazioni o dichiarazioni false ed offensive su un soggetto terzo, non presente alla conversazione anche online che deve coinvolgere due o più persone, idonee a danneggiarne la

reputazione. L’alterazione, divulgazione o diffusione di contenuti online possono talora essere considerati diffamazione e comportare una responsabilità penale e civile.

2. Violazione del copyright: l’alterazione, divulgazione o diffusione di contenuti online può comportare una violazione del copyright se il contenuto alterato viola i diritti esclusivi del titolare. La violazione del copyright può comportare richieste di risarcimento danni e provvedimenti inibitori.
3. Interferenza illecita: l'interferenza illecita si verifica quando un individuo interferisce intenzionalmente con i rapporti commerciali o contrattuali di un'altra persona. L’alterazione dei contenuti online, come l'alterazione di una recensione o di una valutazione di un prodotto, possono essere considerati un'interferenza illecita e comportare una responsabilità civile.

L’attività di alterazione di contenuti online possono anche comportare gravi danni alla reputazione di chi ne è vittima.

I contenuti alterati possono infatti diffondersi rapidamente sui social media e su altre piattaforme online, causando pubblicità negativa e perdita di credibilità; questa tipologia di danno può essere difficile da eliminare e può avere conseguenze di lunga durata.

3.2.1 Conseguenze legali in Italia

Anche in Italia, l'alterazione di documenti informatici può costituire un reato in base all'articolo 491-bis del Codice Penale, che ne punisce la manipolazione fraudolenta

Alla alterazione, manipolazione e divulgazione non autorizzata di contenuti informatici possono essere applicate anche altre normative di settore, come la legge sul diritto d'autore, mentre in taluni casi l’uso dello strumento pubblico dei social per commettere un reato ne costituisce un’aggravante, come nel caso della diffamazione (art. 595 C.P.).

Più in generale i cosiddetti “cyber crimes”, ovvero reati informatici, sono stati introdotti nel Codice Penale dalla Legge n. 547/1993 e, come dalla stessa norma indicato, sono commessi da “chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno”.

Le conseguenze legali per tali reati possono essere molto serie. In caso di condanna, il colpevole potrebbe essere soggetto a una pena detentiva, una multa o entrambe. Inoltre, il colpevole potrebbe essere ritenuto civilmente responsabile per i danni causati alla persona o all'ente vittima del reato.

In ogni caso, al di là della rilevanza penale, il soggetto che ha subito l'alterazione dei contenuti online può intentare una causa civile per ottenere il risarcimento dei danni subiti.

L'autore dell'illecito potrebbe quindi essere obbligato a pagare una somma di denaro per risarcire i danni economici, ed a volte anche quelli morali, causati dalla manipolazione fraudolenta dei dati informatici.

In generale, le conseguenze legali per "cyber crimes" in Italia sono molto serie e possono includere sia pene detentive che multe, oltre al risarcimento dei danni subiti dalla parte lesa.

Conclusioni

La distorsione digitale, rappresentata dall'alterazione dei contenuti online, è un fenomeno complesso che ha avuto un impatto significativo sulla società contemporanea.

Nel corso di questa tesi, abbiamo esaminato i caratteri generali dell'alterazione dei contenuti online, concentrandoci principalmente sul fenomeno delle fake news. Abbiamo esaminato le cause alla base della produzione delle fake news e gli effetti negativi che esse hanno sulla disinformazione. Inoltre, abbiamo analizzato le fasi principali della creazione e diffusione di una fake news. Un aspetto interessante che è emerso durante la nostra ricerca è stato il potenziale ruolo della tecnologia blockchain come possibile soluzione per contrastare le fake news. La tecnologia blockchain offre una maggiore trasparenza e tracciabilità delle informazioni, riducendo così la possibilità di manipolazioni e frodi. Tuttavia, è importante sottolineare che l'implementazione di soluzioni basate su blockchain richiede un impegno collettivo da parte delle istituzioni, delle aziende e degli utenti stessi.

Nel secondo capitolo, abbiamo esaminato diversi esempi di alterazione dei contenuti online. La disinformazione online è uno dei problemi più diffusi, con notizie false che vengono create e diffuse con l'intento di influenzare l'opinione pubblica. Abbiamo anche esplorato il fenomeno dei deepfake, che rappresenta un livello avanzato di manipolazione dei contenuti, consentendo la creazione di video e audio falsi che sembrano autentici. Inoltre, abbiamo esaminato la manipolazione di immagini online, la creazione di siti web falsi e la modifica di post sui social media. Sono stati presentati esempi concreti di come questi tipi di alterazione dei contenuti online siano stati utilizzati per scopi fraudolenti e manipolatori.

Nel terzo capitolo, ci siamo concentrati sulle conseguenze economiche e legali dell'alterazione dei contenuti online. L'impatto economico è significativo, con danni sia per le aziende che per i consumatori. Le aziende possono subire perdite finanziarie a causa della diffusione di informazioni false che danneggiano la loro reputazione e i loro prodotti. I consumatori possono essere truffati o ingannati attraverso siti web falsi o annunci fraudolenti.

Dal punto di vista legale, abbiamo analizzato le conseguenze giuridiche dei reati di alterazione dei contenuti online, con un focus specifico sul contesto italiano. Le sanzioni e le pene variano a seconda del tipo di reato commesso, ma è evidente che l'aspetto legale è un

fattore importante nella lotta contro l'alterazione dei contenuti online.

La distorsione digitale rappresenta una sfida complessa per la società contemporanea. L'alterazione dei contenuti online, in particolare il fenomeno delle fake news, ha un impatto significativo sulla disinformazione e sulla manipolazione dell'opinione pubblica.

È quindi fondamentale affrontare questo problema in modo collaborativo, coinvolgendo istituzioni, aziende e utenti; sono necessarie misure tecniche, regolamentari e di alfabetizzazione digitale per combattere la distorsione digitale.

Dal punto di vista tecnico, è importante sviluppare algoritmi di intelligenza artificiale in grado di identificare e filtrare le informazioni distorte.

Le piattaforme online devono assumersi la responsabilità di combattere la diffusione delle fake news attraverso l'implementazione di algoritmi di rilevamento delle informazioni false e la promozione di contenuti affidabili.

Inoltre, è essenziale migliorare la trasparenza degli algoritmi utilizzati dalle piattaforme per la selezione dei contenuti, in modo che gli utenti possano comprendere come vengono presentate loro le informazioni e quali possono essere le distorsioni introdotte.

Dal punto di vista regolamentare, i governi devono adottare misure per contrastare la distorsione digitale.

Queste possono includere leggi che obblighino le piattaforme a eliminare o etichettare i contenuti falsi, sanzioni per la diffusione volontaria di informazioni false e la promozione di standard etici per il giornalismo online; è però importante che tali misure siano equilibrate e rispettino la libertà di espressione, evitando di diventare strumenti di censura.

Inoltre, è necessario investire nell'alfabetizzazione digitale; gli utenti devono essere educati a valutare criticamente le informazioni che incontrano online, a riconoscere le fonti affidabili e a verificare la veridicità delle notizie.

L'alfabetizzazione digitale dovrebbe essere parte integrante dei programmi scolastici e degli sforzi educativi per garantire che le persone siano in grado di navigare nel panorama mediatico complesso e identificare la distorsione digitale.

Infine, si è evidenziato come la collaborazione tra istituzioni, aziende e utenti sia fondamentale per affrontare la distorsione digitale; le piattaforme online devono collaborare con le autorità e con gli esperti del settore per sviluppare soluzioni efficaci.

Inoltre, le aziende, i governi e le organizzazioni della società civile devono promuovere la

responsabilità nell'utilizzo dei media digitali e lavorare insieme per contrastare la distorsione digitale.

In conclusione, la distorsione digitale è un problema complesso che richiede un approccio multifattoriale.

Solo attraverso misure tecniche, regolamentari e educative possiamo affrontare efficacemente la diffusione delle fake news e la manipolazione dell'opinione pubblica.

La protezione dell'informazione e della verità è fondamentale per preservare una società informata e democratica.

Sitografia e bibliografia

Senato della repubblica - il Sito Storico, Parlamento Italiano - Disegno di legge S. 2688 - 17ª Legislatura. Available at: https://www.senato.it/leg/17/BGT/Schede/Ddliter/47680.htm.

I reati informatici. (2022) *Il portale giuridico online per i professionisti - Diritto.it*. Available at: https://www.diritto.it/i-reati-informatici/.

Redazione, *Bufale, Pagella Politica*. Available at: https://pagellapolitica.it/bufale.

La fiducia nei media al tempo delle fake news (2020) *CENSIS*. Available at: https://www.censis.it/comunicazione/15%C2%B0-rapporto-censis-sulla-comunicazione/la-fiducia-nei-media-al-tempo-delle-fake-news.

Covid-19 e fake news nei social media (2020) *FBK*. Available at: https://www.fbk.eu/it/press-releases/covid-19-e-fake-news-nei-social-media/.

HKS Misinformation Review (no date) *Misinformation Review*. Available at: https://misinforeview.hks.harvard.edu/.

Home (2023) *First Draft*. Available at: https://firstdraftnews.org/.

Tsang, S.J. *et al.* (2023) *International Fact-Checking Network, Poynter*. Available at: https://www.poynter.org/ifcn/.

Lattari, F. *Ministry of Enterprises and made in Italy, sito del Ministero dello Sviluppo Economico*. Available at: https://uibm.mise.gov.it/index.php/en/lotta-alla-contraffazione/servizi-per-imprese-e-consumatori/tecnologie-anticontraffazione/sot-servizio-orientamento-tecnologie-anticontraffazione/tecnologie-distributed-ledger

Le Strategie di disinformazione online e la Filiera dei Contenuti Fake (2019) *IBC online*. Available at: https://www.ibconline.it/news-eventi/news/le-strategie-di-disinformazione-online-e-la-filiera-dei-contenuti-fake-leggi-il-documento-elaborato-dal-tavolo-tecnico-agcom/.

Law, di D.P. (2022) *Disinformazione online: Il Delicato Rapporto tra social platforms Ed Utenti, Data Protection Law | Privacy e protezione dati personali*. Available at: https://www.dataprotectionlaw.it/2022/05/04/disinformazione-online-il-delicato-rapporto-tra-social-platforms-ed-utenti/.

Dogma Agenzia Investigativa (2021) *Deepfake: Cosa Sono, Come Crearli e come riconoscerli, www.dogma.it*. Dogma Agenzia Investigativa. Available at: https://www.dogma.it/it/news/deepfake--cosa-sono--come-crearli-e-come-riconoscerli.

Carlini, V. (2021) *Deepfake e Video Manipolati: Come funziona il Lato Oscuro dell'intelligenza artificiale, Il Sole 24 ORE*. Available at: https://www.ilsole24ore.com/art/il-lato-oscuro-internet-cosi-vengono-fabbricate-fake-news-ABYjTJaB?refresh_ce=1.

La Tempesta Perfetta: Social media, fake news e la razionalità limitata. Available at: https://www.researchgate.net/publication/327631448_LA_TEMPESTA_PERFETTA_SOCIAL_MEDIA_FAKE_NEWS_E_LA_RAZIONALITA_LIMITATA_DEL_CITTADINO.

Trusted Shops (2023) *Siti di Acquisti Online Falsi e Truffe, Come Smascherarli, Siti di acquisti online falsi e truffe, come smascherarli*. Trusted Shops. Available at: https://business.trustedshops.it/blog/crimine-informatico-siti-falsi-smascherarli.

La truffa dei finti siti con https: Così Si evita la Nuova Trappola del Phishing (2023) *Cyber Security 360*. Available at: https://www.cybersecurity360.it/nuove-minacce/la-truffa-dei-finti-siti-con-https-cosi-si-evita-la-nuova-trappola-del-phishing/.

Vercellotti, A. and Alessandro Vercellotti Avvocato del Digitale (2023) *false recensioni on line: Cosa Si Rischia? Legal for Digital*. Available at: https://legalfordigital.it/reati-informatici/false-recensioni/.

Social e Motori di Ricerca, come la rete influenza le opinioni, *Fastweb.it*. Available at: https://www.fastweb.it/fastweb-plus/digital-magazine/come-influenzare-le-persone-con-social-e-motori-di-ricerca/.

Fake news & manipolazione – bolle di filtraggio, Social Bot E bufale, Fake News & manipolazione – Bolle di filtraggio, social bot e bufale: Giovani e media. Available at: https://www.giovaniemedia.ch/temi/fake-news-manipolazione-bolle-di-filtraggio-social-bot-e-bufale.

Redazione and Authority, *Diritto Dell'informazione by Ruben Razzante*, *Diritto Dell'informazione - Portale di Informazione*. Available at: https://dirittodellinformazione.it/.