DAL SILENZIO ALL'AZIONE
VOL. II

Violenza di Genere Online:
fenomeni, impatti e strategie di
contrasto nel contesto lavorativo

valore D

PERMESSONEGATO

UNA NESSUNA CENTOMILA
FONDAZIONE

DAL SILENZIO ALL'AZIONE
VOL. II

Violenza di Genere Online:
fenomeni, impatti e strategie di
contrasto nel contesto lavorativo

Valore D è la prima associazione di imprese in Italia – oltre 400 ad oggi, per un totale di più di due milioni di dipendenti e un giro d'affari aggregato di oltre 500 miliardi di euro – che dal 2009 è impegnata a costruire un mondo professionale senza discriminazioni, in cui l'uguaglianza di genere e la cultura dell'inclusione supportano l'innovazione, il progresso e la crescita delle organizzazioni e del nostro Paese. L'associazione è nata dall'incontro tra dodici manager di altrettante aziende virtuose: parliamo di AstraZeneca, Enel, General Electric, Johnson&Johnson, IKEA, Intesa Sanpaolo, Luxottica, McKinsey & Company, Microsoft, Standard&Poor's, UniCredit e Vodafone. Valore D affianca le aziende associate fornendo know-how e strumenti efficaci per una strategia di Diversity & Inclusion, perché le aziende con maggiore diversità affrontano meglio le sfide del mercato. Valore D offre inoltre l'opportunità di un confronto interaziendale grazie allo scambio di buone prassi e di un dialogo continuo tra gli associati, in un gioco di squadra che rende Valore D interlocutore di riferimento delle istituzioni e promotore di azioni per lo sviluppo sociale ed economico del Paese.

Contributi a cura di
Nicole Monte, Vicepresidente
Permesso Negato e partner 42LF

Coordinamento editoriale
Team Public Affairs Valore D
Team Centro Studi Valore D
Fondazione Una Nessuna Centomila

Editing
Simone Marcelli Pitzalis

Progetto Grafico
Team Comunicazione Valore D

Editore
Valore D

In collaborazione con

Indice

Prefazione Valore D e Una Nessuna Centomila

Dal silenzio all'azione: il digitale come nuova frontiera del cambiamento

Affrontare la violenza di genere significa misurarsi con **un fenomeno sistemico**, radicato in disuguaglianze di potere che attraversano ogni ambito della società. Negli ultimi anni abbiamo imparato a riconoscerla nei contesti familiari, relazionali e lavorativi.
Oggi, però, **la violenza si manifesta sempre più spesso in uno spazio che fino a poco tempo fa appariva "altro": il digitale.** Un ambiente che non è separato dalla realtà, ma ne costituisce parte integrante, influenzando profondamente vite, relazioni e scelte personali e professionali.

Come rete di imprese impegnata da sempre sui temi della parità e dell'inclusione, **Valore D** ha scelto, insieme alla **Fondazione Una Nessuna Centomila**, di esplorare questa nuova dimensione. Dopo la prima policy *Dal Silenzio all'Azione*, dedicata alla prevenzione e al contrasto della violenza di genere e domestica nei contesti lavorativi, **abbiamo sentito l'urgenza di estendere il nostro impegno alla violenza di genere online.** Lo facciamo perché crediamo che il mondo del lavoro non possa restare spettatore: deve essere protagonista del cambiamento, anche nel digitale.

Secondo una recente indagine condotta da SWG per Valore D, **l'83% degli italiani considera la violenza di genere online un problema serio**, con effetti concreti sulla salute mentale. **Il 78% la collega alla mancanza di educazione digitale ed emotiva, e il 63% ne riconosce una radice patriarcale.** Tuttavia, molte forme di violenza digitale restano invisibili: meno di quattro italiani su dieci conoscono fenomeni come ***doxing*** o ***sextortion.*** Inoltre, il 64% ritiene che abusi digitali possano verificarsi non solo nella vita privata, ma anche nei contesti di lavoro.

Questi dati ci chiedono di agire e indicano una direzione chiara: **una responsabilità condivisa tra istituzioni, imprese, scuole e piattaforme digitali.** Per questo, insieme all'associazione Permesso Negato – impegnata da anni nel contrasto alla pornografia non consensuale e nel supporto alle vittime – abbiamo realizzato questo nuovo capitolo della policy *Dal Silenzio all'Azione*, interamente dedicato alla violenza di genere online.

Il documento ha un duplice obiettivo: **diffondere consapevolezza in ambito aziendale e offrire strumenti operativi per prevenire, intervenire e proteggere.** Perché il digitale non è un altrove, ma uno spazio in cui si costruiscono fiducia, rispetto e libertà.

Con questo lavoro, Valore D e Fondazione Una Nessuna Centomila rinnovano il loro impegno: **fare cultura contro la violenza di genere, creare alleanze e promuovere azioni concrete.** Perché il cambiamento non può più aspettare. E perché, anche online, è tempo di passare dal silenzio all'azione.

Barbara Falcomer
Direttrice Generale
Valore D

Giulia Minoli
Presidente
Fondazione Una Nessuna Centomila

Introduzione
Permesso Negato

La trasformazione digitale, accelerata da modelli di lavoro agili e da remoto, ha ridefinito il concetto stesso di "luogo di lavoro". Le pareti dell'ufficio sono state sostituite dagli schermi dei nostri dispositivi, e le interazioni professionali si sono spostate su piattaforme di comunicazione istantanea, social network e spazi virtuali. Questa evoluzione, ricca di opportunità in termini di flessibilità e collaborazione, ha però anche eroso i confini tradizionali tra la sfera privata e quella lavorativa, creando nuove superfici di attacco e nuove, insidiose vulnerabilità. Le mura che possono imprigionare, ferire e limitare non sono più soltanto quelle fisiche della casa: oggi esistono anche mura digitali, in cui la violenza di genere ha trovato un terreno fertile per manifestarsi in forme inedite.

PermessoNegato, associazione specializzata nel contrasto alla violenza online e alla pornografia non consensuale, nell'intersezione tra diritto e nuove tecnologie, si confronta con il dolore delle vittime di abusi online. Questo addendum nasce con lo scopo di fornire alle aziende una mappa aggiornata e strumenti concreti per confrontarsi con questa nuova realtà. L'obiettivo è estendere l'efficace approccio **ISSA** (**Informare, Svelare, Sostenere, Amplificare**) al dominio digitale, affinché nessuna azienda si trovi impreparata e nessuna dipendente si senta sola di fronte alla violenza online.

È fondamentale chiarire sin da subito che **la dimensione digitale del fenomeno non rende la violenza di genere online meno grave**. Al contrario, è una manifestazione diretta e brutale della violenza di genere tout court, radicata nella medesima cultura della disuguaglianza e negli stessi squilibri di potere che il manuale "Dal Silenzio all'Azione" ha lucidamente analizzato.
La tecnologia, in questo contesto, non è la causa ultima del problema, ma agisce come un formidabile amplificatore di violenza, odio e controllo. Questa forma di violenza opera su un continuum che va dall'hate speech al revenge porn, dal cyberstalking alla diffamazione professionale.

Ciò che la rende particolarmente distruttiva sono le caratteristiche che la tecnologia le conferisce:

La pervasività
che annulla ogni spazio sicuro rendendo la vittima raggiungibile ovunque;

L'amplificazione
per cui un singolo contenuto può raggiungere un pubblico illimitato;

La permanenza
poiché ciò che viene pubblicato online è quasi impossibile da rimuovere.

L'analisi dell'attuale panorama della violenza di genere online rivela l'esistenza di un complesso ecosistema digitale strutturato su molteplici piattaforme e canali, caratterizzato da livelli progressivi di occultamento e sofisticazione tecnica. **Tale architettura criminale si articola principalmente attraverso tre dimensioni interconnesse: i canali Telegram, i forum accessibili dal web tradizionale e le reti del dark web**, ciascuna delle quali presenta specifiche modalità operative e gradi differenti di accessibilità.

Telegram, per esempio, è popolato di canali dove viene condivisa pornografia non consensuale, anche di minori. Questo si spiega attraverso le caratteristiche tecniche della piattaforma, che garantisce crittografia end-to-end, possibilità di creare canali con migliaia di membri, funzioni di auto-distruzione dei messaggi e sostanziale impunità operativa.
Il gruppo Facebook "Mia Moglie" con 30mila iscritti italiani è solo un pezzo di un problema che ha sede principalmente su Telegram, dove la violenza digitale continua anche dopo

le chiusure dei gruppi più visibili sui social network tradizionali.
"Mia moglie" era un gruppo pubblico aperto su Facebook nel 2019, ma realmente attivo da maggio 2025, su cui erano condivise foto intime e private di mogli e compagne, a loro insaputa, con commenti violenti e sessisti. Meta ha chiuso il gruppo, ma il caso rappresenta paradigmaticamente le dinamiche di migrazione delle comunità violente tra piattaforme diverse: è infatti bene chiarire che in seguito a segnalazioni e chiusure di singole pagine o gruppi, solitamente emergono nuovi gruppi o se ne riattivano altri sopiti da tempo, evidenziando la natura sistemica e resiliente di tali reti criminali.

Parallelamente, l'esistenza di forum specializzati come Phica.eu ha dimostrato la presenza di **infrastrutture dedicate esclusivamente alla sistematizzazione della violenza digitale**. La Polizia Postale ha sequestrato il sito Phica.eu, finito al centro delle denunce di decine di donne italiane. Il sito conteneva foto di donne, anche note, pubblicate online senza il loro consenso e accompagnate da commenti sessisti. L'analisi investigativa ha rivelato un modello di business criminale particolarmente insidioso: ad alcuni utenti del forum era stato chiesto di pagare un contributo per essere eliminati dagli iscritti, con richieste economiche che potevano raggiungere fino a 1000 euro per rimuovere foto rubate, configurando ipotesi di estorsione sistematica.

La dimensione del dark web rappresenta il livello più sofisticato e pericoloso dell'ecosistema della violenza digitale, caratterizzato da mercati specializzati, sistemi di pagamento anonimi e reti di distribuzione internazionali. All'interno di queste reti criptate operano veri e propri marketplace dedicati alla compravendita di materiale non consensuale, servizi di doxing personalizzato, commissioni per la creazione di deepfake pornografici e piattaforme per la coordinazione di campagne di molestie collettive. L'accessibilità di tali servizi attraverso criptovalute e l'anonimato garantito dai protocolli di crittografia creano un ambiente sostanzialmente immune alle tradizionali attività di polizia giudiziaria.

L'interconnessione tra questi tre livelli genera **un effetto moltiplicatore della violenza**, dove contenuti inizialmente condivisi su piattaforme mainstream migrano progressivamente verso canali sempre più occultati, subendo processi di amplificazione, manipolazione e commercializzazione.

Tale dinamica trasforma la violenza episodica in violenza sistematica, la vittimizzazione individuale in industria criminale, e la misoginia occasionale in economia parallela della degradazione femminile.

Le indagini condotte dalla Polizia Postale e dalle autorità europee hanno documentato l'esistenza di vere e proprie ***supply chain* della violenza digitale**, caratterizzate da ruoli specializzati: raccoglitori di materiale, amministratori tecnici, moderatori di contenuti, operatori di marketing criminale e gestori finanziari. Dall'Italia alla Corea del Sud, dagli Stati Uniti alla Spagna, sempre più gruppi online condividono immagini intime senza consenso. Tra *deepfake*, chat chiuse e normative in evoluzione, il fenomeno globale mette a rischio la dignità delle donne, rendendo necessari approcci investigativi e normativi transnazionali per contrastare efficacemente questa forma di criminalità digitale evoluta.

In questo quadro, **la cooperazione tra pubblico e privato rappresenta uno snodo cruciale per la prevenzione e il supporto alle vittime**; dunque, per le aziende, il primo passo è comprendere che il perimetro di questa violenza permea anche l'ecosistema lavorativo digitale. Ignorare questa realtà significa esporre le proprie persone a rischi concreti che impattano sulla loro salute, sulla loro carriera e, di conseguenza, sulla produttività e sulla reputazione dell'intera organizzazione. Questo capitolo fornirà gli strumenti per passare dalla necessaria consapevolezza all'azione strategica.

Il benessere digitale nel contesto della violenza di genere online: l'ambiente lavorativo

Il concetto di **benessere digitale** assume una rilevanza particolare nell'analisi della violenza di genere online in ambito lavorativo, configurandosi come **elemento cardine per comprendere gli impatti sistemici di tali fenomeni sull'individuo e sull'organizzazione.** Secondo l'Organizzazione Mondiale della Sanità, la salute è "uno stato di completo benessere fisico, mentale e sociale e non semplicemente l'assenza di malattia o infermità", definizione che assume contorni specifici quando applicata agli ambienti digitali contemporanei nel contesto lavorativo.

La digitalizzazione massiva degli ambienti lavorativi ha, infatti, creato nuove dimensioni di vulnerabilità:

Secondo il rapporto UNESCO *"Combatting Online Violence Against Women and Girls: A Worldwide Wake-Up Call"*, **il 73% delle donne** ha già subito o sperimentato qualche forma di **violenza online**, evidenziando la pervasività del fenomeno negli spazi digitali contemporanei.

Questo dato acquisisce particolare significato nel contesto lavorativo digitale, dove **le tecnologie digitali presentano varie sfide**, come cambiamenti nei ruoli lavorativi, spostamento dei dipendenti, aumento del carico di lavoro e confini lavorativi sfumati.

Il benessere digitale sul posto di lavoro non può essere separato dalla comprensione del fenomeno del "***technostress***", definito come le conseguenze negative della tecnologia digitale sui lavoratori. Alcuni studi hanno dimostrato **un impatto negativo dell'uso eccessivo di dispositivi che porta a un declino nei tassi di performance, effetti sui pattern del sonno e riduzione nei risultati lavorativi**, causando così ostacoli nel liberare il massimo potenziale di un individuo.

La dimensione intersezionale del benessere digitale emerge chiaramente quando si considerano le specificità dei gruppi vulnerabili. Le molestie sono di particolare preoccupazione per la coorte studiata poiché **i gruppi di minoranze sessuali sono intrinsecamente ad alto rischio di scarso benessere psicosociale** a causa di fattori legati allo stress minoritario, alla stigmatizzazione e all'omofobia interiorizzata. Questa vulnerabilità si amplifica negli ambienti lavorativi digitali, dove le dinamiche di potere preesistenti si intersecano con le nuove forme di violenza tecnologicamente mediate.

L'impatto sulla produttività e sul benessere organizzativo è documentato in modo crescente dalla ricerca accademica. I dati suggeriscono che **l'intensità della tecnologia digitale sul workplace, come riflesso nelle esperienze delle richieste lavorative digitali, può compromettere la salute fisica e mentale dei lavoratori.** Questo fenomeno si manifesta con particolare intensità quando le donne subiscono forme di violenza online che compromettono non solo la loro sicurezza personale, ma anche la loro capacità di partecipare pienamente alla vita lavorativa digitale.

La violenza di genere online nel contesto lavorativo crea quello che può essere definito un "***digital wellness deficit***" - una sorta di condizione lavorativa in cui **l'esposizione costante a contenuti ostili, molestie e discriminazioni digitali compromette sistematicamente il benessere psicofisico del lavoratore.**
Le implicazioni per le strategie aziendali di benessere digitale sono molteplici e richiedono un approccio olistico che integri la prevenzione della violenza di genere online con politiche più ampie di *digital wellness*.

Le organizzazioni devono riconoscere che il benessere digitale dei propri dipendenti non può essere garantito attraverso semplici misure tecniche di sicurezza informatica, ma richiede **un approccio sistemico** che affronti **le dinamiche culturali, le asimmetrie di potere e i bias algoritmici** che possono amplificare fenomeni di violenza e discriminazione.

Dunque, investimenti mirati nel benessere digitale, particolarmente attraverso la lente della prevenzione della violenza di genere online, **non solo migliorano il clima lavorativo e la retention dei talenti, ma contribuiscono anche alla performance organizzativa complessiva.**

In questo contesto e per tutte queste ragioni, il presente documento ha in animo di supportare le aziende nella promozione del benessere digitale, che si configura non come un optional etico, ma come **una necessità strategica per le organizzazioni che intendono prosperare nell'era della digitalizzazione del lavoro**, garantendo al contempo ambienti inclusivi e sicuri per tutti i dipendenti, indipendentemente dal genere e dall'identità.

Parte I
Inquadramento del fenomeno

Per poter contrastare efficacemente la violenza di genere online, è indispensabile prima di tutto conoscerla, definirla e comprenderne i meccanismi. Come evidenziato nel manuale "Dal Silenzio all'Azione", creare un linguaggio comune e una comprensione condivisa del fenomeno è il primo, fondamentale passo per costruire una cultura del rispetto e della sicurezza.

Questa sezione si propone di inquadrare le principali manifestazioni della violenza di genere online, partendo dalla sua forma più diffusa e pervasiva: il discorso d'odio.

Hate Speech di genere

Il discorso d'odio basato sul genere, o *hate speech* di genere, rappresenta una delle porte d'accesso più comuni alla violenza online. In generale si definisce "discorso d'odio" o "hate speech" non una semplice "critica" o un "insulto", ma una forma di espressione mirata a promuovere, istigare e giustificare l'odio, la discriminazione e la violenza contro una persona o un gruppo di persone unicamente a causa di specifiche caratteristiche identitarie. **Nel contesto oggetto di analisi, esso si rivolge in modo sistematico e sproporzionato contro le donne.**

Lo scopo primario dell'*hate speech* di genere non è avviare un dibattito, per quanto aspro, ma è **ridurre la donna a un oggetto, deumanizzarla e negare la sua legittimità a occupare uno spazio, sia esso fisico o digitale.** Serve a "punire" le donne che trasgrediscono i ruoli di genere tradizionali: quelle che esprimono opinioni, che detengono posizioni di potere, che parlano di politica, di economia o di scienza. È uno strumento violento volto a intimidire, umiliare e, in ultima analisi, a silenziare le voci femminili, riaffermando un modello di potere squilibrato.

Focus sulle tecnologie: piattaforme, algoritmi e meccanismi di diffusione

La violenza del discorso d'odio di genere viene amplificata in modo esponenziale dalla tecnologia. Le piattaforme su cui si manifesta sono molteplici e interconnesse, rendendo il fenomeno endemico.
Non parliamo solo dei social media più noti come X (precedentemente Twitter), Facebook, Instagram e TikTok, ma anche delle sezioni commenti di YouTube, dei forum anonimi come Reddit, delle chat utilizzate nelle piattaforme di gaming online e, punto focale per le aziende, dei social network professionali come LinkedIn, che non sono immuni da queste dinamiche.

Il primo meccanismo di diffusione è guidato dagli utenti stessi. Un attacco può iniziare con un singolo commento o post offensivo, per poi diffondersi a macchia d'olio attraverso condivisioni, retweet e screenshot che ne moltiplicano la visibilità.
Spesso questi attacchi non sono spontanei ma coordinati. **Gruppi di utenti, talvolta organizzati in chat private, si accordano per colpire simultaneamente un unico bersaglio (una pratica nota come *brigading* o *dogpiling*)**, sommergendola di insulti e minacce per renderle impossibile qualsiasi interazione e per intimidirla fino a costringerla di fatto al silenzio.

Tuttavia, **il meccanismo più potente e insidioso è quello governato dagli algoritmi delle piattaforme.** Questi sistemi non sono affatto neutrali rispetto al flame generato dall'hate speech. In generale gli algoritmi sono progettati con un obiettivo primario: massimizzare il tempo di permanenza dell'utente e l'interazione (*engagement*), ovvero il numero di "mi piace", commenti e condivisioni.
I contenuti controversi, scioccanti e carichi d'odio generano, per loro natura, un altissimo livello di *engagement*. Di conseguenza, l'algoritmo stesso, seguendo la sua programmazione, può finire per promuovere attivamente il discorso d'odio, mostrandolo a un numero sempre maggiore di utenti e aumentandone la portata virale.

Questo processo di **amplificazione algoritmica** crea le cosiddette "camere dell'eco" (*echo chambers*) e "bolle di filtraggio" (*filter bubbles*), in cui l'algoritmo tende a mostrare a ogni utente contenuti simili a quelli con cui ha interagito in passato.

Dunque, l'utente che interagisce con contenuti misogini riceve dall'algoritmo un numero crescente di proposte affini, rimanendo intrappolato in una spirale di contenuti progressivamente più estremi. Questo non solo rinforza i suoi pregiudizi, ma normalizza l'odio, trasformandolo da un'opinione deviante a una visione del mondo condivisa e accettata all'interno della sua "bolla".

Nonostante ciò, è importante sottolineare che il fenomeno dell'hate speech nelle piattaforme digitali, pur rappresentando una delle sfide più complesse dell'era digitale, è un tema che vede come protagoniste anzitutto le piattaforme, impegnate a progettare una migliore

esperienza utente. I Policy maker delle principali piattaforme social (Meta, Google, TikTok) sono coscienti che i sistemi di raccomandazione algoritmica delle piattaforme social sono governati da questo meccanismo intrinseco che rischia di creare un circolo vizioso e dunque un ambiente digitale insostenibile, in cui gli algoritmi guidano gli utenti verso contenuti progressivamente più estremi, alimentando echo chamber che rafforzano pregiudizi esistenti e facilitano la radicalizzazione delle posizioni.

Quasi tutte le piattaforme hanno dunque investito considerevolmente negli ultimi anni per contrastare questo fenomeno attraverso un approccio multidimensionale che combina intelligenza artificiale e interventi di moderazione umana. Per individuare l'*hate speech* su Facebook e Instagram, per esempio, viene impiegata una combinazione di segnalazioni degli utenti e strumenti tecnologici, come i sistemi automatizzati che già nel 2019 riuscivano a rilevare l'80% dei contenuti d'odio prima ancora che venissero segnalati.

I numeri dell'enforcement sono significativi:

Secondo i dati più recenti, **Meta ha rimosso proattivamente 346 milioni di contenuti** nelle categorie hate speech, bullismo e molestie nel terzo trimestre del 2024, dimostrando l'ampiezza dell'impegno nell'identificazione e rimozione di contenuti problematici.

Tuttavia, l'efficacia di questi sistemi presenta ancora limitazioni significative, particolarmente evidenti nell'approccio algoritmico alla moderazione.

Nel primo trimestre del 2024, **148.000 contenuti rimossi per hate speech sono stati successivamente ripristinati**, di cui 145.000 attraverso processi automatici, evidenziando i margini di errore dei sistemi automatizzati.

Inoltre, alcuni studi hanno dimostrato disparità nell'applicazione delle politiche, mostrando come il 55% dei contenuti segnalati dagli utenti come più dannosi fosse diretto contro sole quattro minoranze: persone nere, mussulmane, ebree e comunità LGBTQIA+, rivelando così bias sistemici che richiedono interventi mirati.

L'impatto di questi meccanismi digitali sul contesto lavorativo è diretto e concreto. Un dipendente che viene progressivamente radicalizzato all'interno di una di queste bolle digitali può facilmente trasportare queste attitudini tossiche e discriminatorie sul luogo di lavoro, manifestandole nelle chat aziendali, durante le riunioni o nelle interazioni quotidiane con le colleghe. Allo stesso modo, una campagna d'odio online diretta contro una manager o una professionista dell'azienda può avere ripercussioni devastanti sulla sua salute psicofisica, sulla sua produttività e sulla reputazione dell'intera organizzazione, che ha il dovere di garantirne la sicurezza.

Inquadramento normativo

Quadro Europeo (DSA, DMA, Direttiva e-Commerce), Normativa Italiana (Codice Rosso), Giurisprudenza di riferimento

Il mondo digitale non è uno spazio senza regole. Sebbene la libertà di espressione sia un diritto fondamentale imprescindibile per l'interazione tra utenti, essa non è mai assoluta e trova il suo limite nel rispetto della dignità e della sicurezza altrui. Sia la legislazione europea che quella internazionale si stanno muovendo con decisione verso un modello che impone maggiori responsabilità alle piattaforme.

Il cardine della nuova architettura normativa europea è il **Digital Services Act (DSA), o Regolamento sui Servizi Digitali.** Questo Regolamento ha l'obiettivo di creare uno spazio online più sicuro e trasparente, imponendo a tutte le piattaforme digitali obblighi stringenti per contrastare la diffusione di contenuti illegali, incluso l'hate speech di genere. Le piattaforme devono predisporre meccanismi semplici per la segnalazione e agire "senza indebito ritardo" per rimuovere tali contenuti, spostando la responsabilità dal solo utente alla piattaforma stessa. Accanto al DSA, il **Digital Markets Act (DMA)** mira a regolare il potere economico delle grandissime piattaforme online, promuovendo un mercato digitale più equo.

In Italia, non esiste una singola legge specificamente dedicata all'"*hate speech*", ma il fenomeno viene combattuto attraverso un insieme di norme penali. **Il reato più frequentemente contestato è quello di diffamazione, previsto dall'articolo 595 del codice penale**, con un'aggravante specifica per l'uso di Internet. In molti casi, le espressioni d'odio possono integrare anche reati più gravi, come la minaccia, lo stalking o la violenza privata.

Un riferimento importante è la Legge n. 69 del 2019, nota come **"Codice Rosso"**. Sebbene nata per la violenza domestica, ha introdotto nell'ordinamento italiano il reato di cui all'art. 612 ter c.p. "Diffusione illecita di immagini o video sessualmente espliciti", che si approfondirà nel prosieguo.

La giurisprudenza italiana, inclusa quella della Corte di Cassazione, ha svolto un ruolo chiave nel definire le responsabilità. Le sentenze degli ultimi anni hanno progressivamente affermato che i gestori di piattaforme online hanno un dovere di controllo e di intervento (*duty of care*) nel momento in cui vengono a conoscenza della presenza di un contenuto illecito. La mancata rimozione di un commento diffamatorio, a seguito di una segnalazione, può comportare una responsabilità diretta per il gestore. Inoltre, le corti riconoscono costantemente la particolare gravità della diffamazione online, a causa della sua capacità di diffusione incontrollata e della sua permanenza nel tempo.

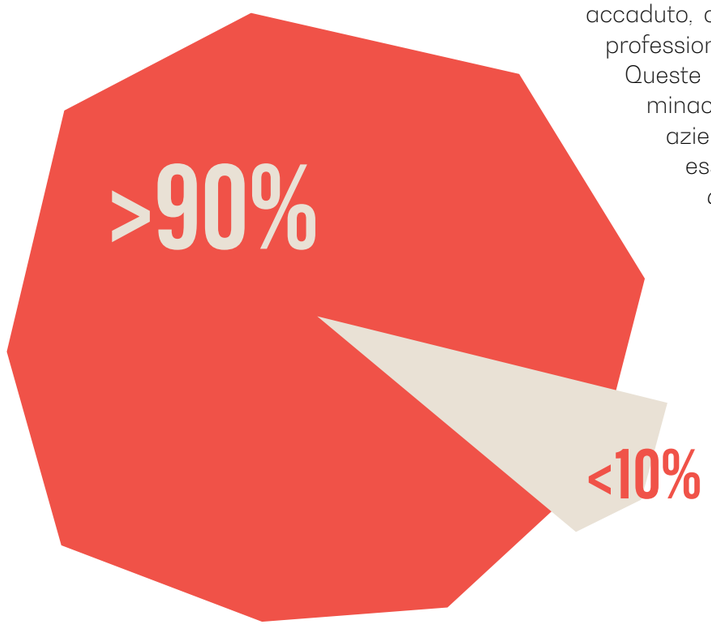
Pornografia non consensuale e Image-Based Sexual Abuse

L'abuso sessuale basato su immagini (in inglese, **Image-Based Sexual Abuse - IBSA**) costituisce una violazione profonda e intima. Questo termine descrive correttamente il fenomeno come **una forma di abuso sessuale che non richiede contatto fisico, ma che utilizza immagini e video per umiliare, controllare e violare una persona.** Il cuore di questa violenza è la diffusione di immagini intime non consensuali (**NCII**).
Anche se un'immagine è stata creata consensualmente, la sua successiva distribuzione a terzi senza il permesso della persona raffigurata costituisce una grave violazione.

Focus sulle tecnologie: *deepfake* e tecnologie di manipolazione, *revenge porn* e *sextortion*, Non-Consensual Intimate Images (NCII)

All'interno della macrocategoria dell'IBSA, è essenziale distinguere due fenomeni: il cosiddetto "***revenge porn***" e la "***sextortion***". Il *revenge porn* consiste nella *distribuzione* effettiva di immagini o video intimi per vendetta o umiliazione. La *sextortion*, invece, è una forma di estorsione che si basa sulla minaccia di distribuire tale materiale per costringere la vittima a fornire denaro, favori sessuali o altre immagini.
Questi fenomeni sono profondamente caratterizzati dal genere. I dati dimostrano che, per quanto riguarda il c.d. *revenge porn* e la diffusione illecita di contenuti intimi:

La stragrande maggioranza delle vittime (oltre il 90%) è di sesso femminile, mentre la quasi totalità dei perpetratori è di sesso maschile.



Diverso è per la cd. Sextortion per cui le vittime sono in prevalenza maschili.

La diffusione di materiale intimo, sia che abbia lo scopo della ripicca sia che avvenga per superficialità o mera goliardia, non si caratterizza per essere un crimine neutro, ma al contrario rappresenta una specifica manifestazione della **violenza di genere**, utilizzata come strumento di controllo misogino.

Oggi, l'abuso è entrato in una nuova e ancora più terrificante era, quella dei ***deepfake***. Un *deepfake* è un video o un'immagine altamente realistica, ma completamente falsa, creata utilizzando l'intelligenza artificiale. Attraverso software sempre più accessibili, è possibile sovrapporre il volto di una persona (ad esempio, una collega di lavoro) al corpo di un'altra in un contenuto pornografico, creando un falso credibile e devastante.

Le implicazioni dei *deepfake* sono profonde. Questa tecnologia rende possibile vittimizzare chiunque, anche una persona che non ha mai scattato un'immagine intima di sé. Il materiale manipolato può essere indistinguibile da un video autentico, rendendo estremamente difficile per la vittima difendersi. Si crea così una nuova forma di "**aggressione digitale**" che può annientare la reputazione di una persona, basandosi su un evento che non è mai accaduto, con conseguenze psicologiche e professionali incalcolabili.

Queste tecnologie rappresentano una minaccia diretta anche per il contesto aziendale, dove una dipendente può essere facilmente bersaglio di un *deepfake* creato da un collega o da un aggressore esterno.

Framework legale

Art. 612-ter c.p. (diffusione illecita di immagini), Art. 612 quater c.p. Legge sull'AI, la normativa sulla protezione dei dati personali e la tutela del diritto all'immagine, Responsabilità delle piattaforme e nuove forme di tutela

Di fronte a queste nuove forme di violenza, il sistema legale sta evolvendo per offrire tutele più robuste. L'abuso basato su immagini viene sempre più riconosciuto come una grave violazione dei diritti fondamentali della persona.

Il pilastro della normativa italiana, come si è detto, è **l'articolo 612-ter del Codice penale**, introdotto nel 2019 dalla legge "Codice Rosso". Questa norma punisce chiunque diffonda immagini o video a contenuto sessualmente esplicito di una persona senza il suo consenso. **È fondamentale sottolineare che la legge punisce non solo il primo distributore, ma anche chiunque riceva tale materiale e contribuisca a diffonderlo.**
Per un'azienda, questo significa che la condivisione di materiale di questo tipo in un gruppo di lavoro costituisce il compimento di un reato al proprio interno.

Con riferimento ai *deepfake*, la Legge n. 223 del 25-9-2025, che istituisce il quadro nazionale sull'Intelligenza Artificiale mira a introdurre all'interno del Codice penale l'art. 612-quater che propone un nuovo reato, ovvero l'illecita diffusione di contenuti generati o manipolati artificialmente.
La bozza legislativa si articola nella formulazione del nuovo art. 612-quater c.p. che intende punire "chiunque, mediante l'impiego di sistemi di intelligenza artificiale, crei o diffonda contenuti falsi atti a danneggiare la reputazione, la dignità o la vita privata di un individuo, inducendo in errore i destinatari sulla genuinità dei contenuti stessi". La pena prevista può arrivare a 5 anni di reclusione, con aggravanti se la vittima è un minore o se il fine è di lucro o vendetta. Si procede a querela di parte, salvo ipotesi di particolare gravità (minorenni, disabili, autorità pubblica oppure condotta connessa ad altro delitto per cui si procede d'ufficio).

Scopo dichiarato del disegno di legge è **punire in modo specifico la creazione di *deepfake* lesivi, rendendo più agevole l'attività inquirente.** Nello specifico, come già verificatosi per il già menzionato reato di Diffusione illecita di immagini o video sessualmente espliciti (art. 612-ter c.p.), introdotto nel 2019 con Codice Rosso, se venisse introdotta questa norma incriminatrice non sarebbe più necessario inquadrare il fatto come diffamazione, sostituzione di persona o illecito trattamento di dati personali. A tutto questo si aggiunga che nello stesso DDL il Legislatore italiano ha introdotto con l'art. 22 l'attribuzione di una delega al Governo per introdurre nuove fattispecie di reato e modificare la disciplina sulla responsabilità penale, anche per gli enti ai sensi del D.Lgs. 231/2001.

A questa tutela si affianca quella offerta dal **Regolamento Generale sulla Protezione dei Dati (GDPR)**. Un'immagine intima è, a tutti gli effetti, un dato personale e, spesso, un **"dato particolare"** (art. 9 GDPR), meritevole del massimo livello di protezione. La diffusione e l'utilizzo in generale, dunque, può avvenire unicamente sulla base del consenso del soggetto ritratto. Di pari l'ordinamento italiano prevede la tutela dell'immagine (Art. 10 c.c. e artt. 96–97 Legge sul diritto d'autore) nel caso in cui l'abuso digitale sia commesso attraverso l'utilizzo dell'immagine di una persona senza il consenso del soggetto ritratto, ledendone il decoro. Attraverso l'applicazione di queste norme la vittima può chiedere l'immediata cessazione dell'uso illecito e il risarcimento dei danni.

La responsabilità si estende anche alle piattaforme online. **Il Digital Services Act (DSA) europeo ha rafforzato l'obbligo per i social media di agire con celerità per rimuovere le immagini intime non consensuali.** In Italia, il Garante per la Protezione dei Dati Personali ha istituito una procedura d'urgenza che permette alle vittime di segnalare preventivamente il rischio di diffusione, consentendo un intervento proattivo prima che il danno si realizzi.

Altri fenomeni digitali illeciti

Cyberstalking e molestie digitali

La persecuzione reiterata tramite strumenti digitali (monitoraggio social, messaggistica ossessiva, uso di spyware) che genera nella vittima un fondato stato di ansia e paura (art. 612-bis c.p. "Atti Persecutori").
In generale è una condotta spesso sibillina e, se commesso in ambito lavorativo, annienta ogni confine tra vita privata e lavoro, poiché il persecutore può utilizzare canali professionali (e-mail aziendale, LinkedIn) per continuare la molestia, con un impatto devastante sulla concentrazione e la sicurezza della vittima.

Doxxing

Consiste nella **pubblicazione online di dati privati di una persona** (indirizzo, numero di telefono, luogo di lavoro) **per esporla a minacce nel mondo reale.** Trasforma la violenza da digitale a fisica, creando un rischio per la sicurezza non solo della vittima, ma dell'intero luogo di lavoro, che può diventare bersaglio di intrusioni o proteste.

Trolling di genere coordinato

Una strategia di disturbo massiccia e organizzata, attuata da più account, per sabotare le conversazioni online, inquinare i canali di comunicazione di un'azienda o di una professionista e silenziare le voci femminili attraverso un'azione di sfinimento psicologico, danneggiando reputazione personale, brand reputation e gli sforzi di comunicazione.

Parte II
Aspetti psicologici e sociali

Per contrastare in modo strategico ed efficace la violenza di genere online, non è sufficiente mapparne le manifestazioni e comprenderne le conseguenze professionali.
È indispensabile fare un passo ulteriore e più profondo: analizzare le dinamiche psicologiche, sociali e tecnologiche che ne favoriscono la nascita e ne accelerano la diffusione. La violenza digitale non emerge dal nulla; germoglia su un terreno fertile composto da secolari pregiudizi umani e viene nutrita e potenziata da nuovi e potentissimi acceleratori tecnologici.

Comprendere questo intreccio tra la psiche umana e la macchina algoritmica è cruciale per ogni azienda.
Le organizzazioni, infatti, non sono composte da entità astratte, ma da persone, con i loro pregiudizi e i loro schemi mentali. Ignorare come questi bias cognitivi operino e come vengano amplificati dalle piattaforme che usiamo ogni giorno significa combattere una battaglia alla cieca. **Questa sezione si propone di accendere una luce su questi meccanismi, per fornire alle aziende gli strumenti culturali necessari a una prevenzione reale** e non solo di facciata.

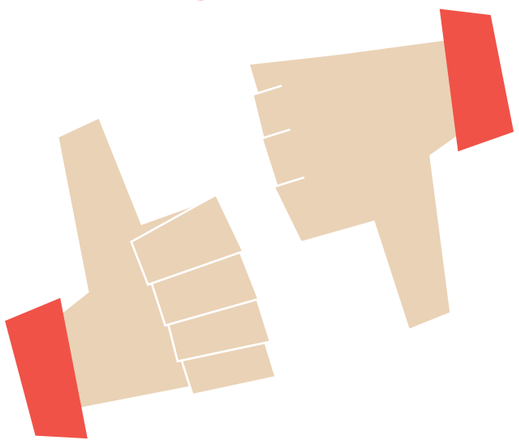
Bias cognitivi e tecnologici

Alla base della violenza di genere online vi è una simbiosi tossica tra i "bug" del pensiero umano - i cosiddetti bias cognitivi, come il bias di conferma o l'illusione di verità - e le caratteristiche strutturali delle piattaforme digitali. Questo incontro amplifica emozioni come paura, frustrazione e bisogno di appartenenza, favorendo processi di disinibizione che rendono più facile esprimere aggressività. In questo modo, **pregiudizi che in altri contesti resterebbero latenti non solo sopravvivono, ma vengono rafforzati, radicalizzati e trasformati in azione violenta.**

Algorithmic bias: come gli algoritmi amplificano stereotipi di genere

Comprendere il funzionamento degli algoritmi è per le aziende una competenza strategica. Un algoritmo non è altro che un insieme di istruzioni e modelli matematici che un sistema informatico segue per eseguire un compito.

Lungi dall'essere neutrali o obiettivi, gli algoritmi sono profondamente **influenzati** dai dati con cui vengono addestrati e dalle scelte di chi li progetta.



Il pregiudizio, o bias, si insinua nell'algoritmo principalmente in due modi. Il primo è attraverso i dati di addestramento. Gli algoritmi imparano analizzando quantità sconfinate di dati prodotti da esseri umani. Se questi dati riflettono i pregiudizi storici della nostra società - per esempio, testi e immagini che associano sistematicamente gli uomini alla leadership e le donne alla cura - l'algoritmo non farà altro che apprendere e riprodurre questi stereotipi su larga scala. Questo meccanismo rafforza i bias già presenti nella mente delle persone, come lo ***stereotype threat***, alimentando convinzioni e comportamenti discriminatori.

Il secondo canale è la progettazione stessa del sistema. I team che sviluppano questi algoritmi sono, ancora oggi, spesso composti in larghissima maggioranza da uomini. Le loro scelte e i loro pregiudizi inconsci possono essere involontariamente "codificati" nelle istruzioni che l'algoritmo seguirà. Qui entra in gioco anche la dimensione psicologica della cecità ai bias: **chi progetta spesso non è consapevole dei propri pregiudizi**, e proprio questa inconsapevolezza li rende ancora più pervasivi.

Un esempio classico di algorithmic bias è visibile nei motori di ricerca. Se per anni una ricerca di immagini per il termine "CEO" ha restituito quasi esclusivamente fotografie di uomini, è perché l'algoritmo ha imparato questa associazione dai contenuti esistenti sul web. Un altro esempio riguarda gli algoritmi di moderazione dei contenuti, che possono essere tarati su pregiudizi sociali, censurando più aggressivamente immagini del corpo femminile rispetto a quelle del corpo maschile.

La conseguenza più grave è che l'algoritmo non si limita a riflettere i pregiudizi esistenti: li amplifica. Creando un ciclo di feedback costante, il sistema rende questi stereotipi onnipresenti, facendoli apparire più "normali" di quanto non siano nella realtà. Questa normalizzazione agisce come un processo di desensibilizzazione: **gli individui si abituano a vedere disparità e stereotipi, fino a considerarli naturali.** Così facendo, si crea un ambiente culturale permissivo per la violenza e per la giustificazione di comportamenti discriminatori. Per un'azienda, questo non è un problema astratto. Le organizzazioni utilizzano sistemi algoritmici in processi critici come il recruiting o la valutazione della performance, e un algoritmo affetto da gender bias può sistematicamente penalizzare le donne, creando discriminazione e vanificando ogni investimento in Diversità e Inclusione. Non a caso, l'AI Act europeo classifica questi sistemi come "ad alto rischio", imponendo alle aziende presidi specifici contro la discriminazione.

Confirmation bias: *echo chambers* e polarizzazione

Il bias di conferma è la nostra naturale inclinazione a cercare, interpretare e ricordare le informazioni che confermano le nostre convinzioni preesistenti, ignorando quelle che le contraddicono. È una scorciatoia mentale che ostacola il pensiero critico e riduce la capacità di mettere in discussione i propri schemi cognitivi.

Gli algoritmi dei social media agiscono come un potentissimo acceleratore di questo bias. Poiché il loro obiettivo primario è massimizzare il nostro tempo di permanenza sulla piattaforma, il modo più semplice per farlo è mostrarci contenuti con cui siamo già d'accordo. Questo meccanismo ci rinchiude progressivamente in "*camere dell'eco*" (*echo chambers*) e "*bolle di filtraggio*" (*filter bubbles*) informative. Si tratta di una forma di rinforzo selettivo, che consolida le credenze preesistenti rendendo sempre più difficile il contatto con informazioni dissonanti.

All'interno di una camera dell'eco, la nostra visione del mondo non viene mai messa in discussione. **Se un individuo nutre lievi pregiudizi misogini, l'algoritmo inizierà a proporgli una dieta costante di contenuti che validano e rafforzano tali pregiudizi.** Le voci alternative o contrarie vengono filtrate e progressivamente escluse. Ciò alimenta la cognizione motivata (*motivated reasoning*): la tendenza a elaborare le informazioni in modo da difendere la propria identità e i propri valori.

L'effetto di questo isolamento informativo non è solo una conferma, ma **una polarizzazione**: le opinioni diventano più rigide ed estreme.

All'interno della bolla, si sviluppa un forte senso di appartenenza al gruppo ("noi") e una crescente ostilità verso chiunque la pensi diversamente ("loro"). Questo dinamismo è spiegabile con **la teoria dell'identità sociale**, così come teorizzata da Henri Tajfel e John Turner: la distinzione tra *ingroup* e *outgroup* accentua il favoritismo verso il proprio gruppo e la demonizzazione dell'altro. Tuttavia, l'ampiezza dell'effetto varia per piattaforma e contesto: in alcuni casi, l'esposizione a contenuti opposti può persino irrigidire le posizioni (effetto boomerang).

È in questo passaggio dalla polarizzazione all'ostilità che si crea il legame con la violenza. Un gruppo di persone intrappolate in un'eco-camera misogina può arrivare ad aumentare il rischio di giustificazione di azioni di violenza collettiva, come campagne di trolling, contro le donne che vengono identificate come il "nemico". Questo fenomeno ha implicazioni dirette sulla cultura aziendale. Un dipendente immerso in una di queste bolle informative avrà enormi difficoltà a collaborare in modo costruttivo con le colleghe e sarà profondamente resistente a qualsiasi iniziativa di formazione sulla Diversità e l'Inclusione.

Victim blaming: bias nella percezione delle vittime

Il *victim blaming*, ovvero la tendenza a colpevolizzare la vittima, è uno dei bias cognitivi più dolorosi e dannosi. Consiste nel ritenere la persona che ha subito un abuso, in tutto o in parte, responsabile per ciò che le è accaduto. Questo meccanismo nasce da un profondo bisogno psicologico di autodifesa, noto come "Ipotesi del mondo giusto".

L'Ipotesi del mondo giusto è la credenza, spesso inconscia, che il mondo sia un luogo equo dove le persone ottengono ciò che meritano. Se una donna subisce una violenza, è psicologicamente più rassicurante pensare che "deve aver fatto qualcosa per provocarla" piuttosto che accettare la terrificante realtà che una cosa orribile potrebbe accadere a chiunque in modo arbitrario. Questo meccanismo è legato anche al bisogno di controllo: credere che l'ordine morale sia prevedibile riduce l'ansia, ma a costo di distorcere la percezione della vittima.
Nel contesto della violenza di genere online, il victim blaming si manifesta in una serie di frasi tipiche che spostano il focus dall'aggressore alla vittima, come:

"Perché ha pubblicato **quella foto?**"

oppure

"Se non volessi essere molestata, **non dovresti stare sui social media**"

Questo meccanismo è potentemente amplificato dagli stereotipi di genere radicati nella nostra cultura, che hanno sempre esercitato un controllo più stringente sul comportamento e l'espressione delle donne.

L'impatto sulla vittima è devastante. Il victim blaming infligge quella che viene definita vittimizzazione secondaria: **la donna viene traumatizzata una seconda volta, non dall'aggressore, ma dalla reazione indifferente o accusatoria della società.** Questo genera in lei sentimenti di vergogna, colpa e isolamento, e la rende estremamente riluttante a denunciare l'abuso. Inoltre, la combinazione di colpa interiorizzata e isolamento sociale favorisce sintomi depressivi, ansiosi e post-traumatici.

Questo bias tossico si manifesta con forza anche all'interno del contesto lavorativo, nei commenti dei colleghi o nelle domande poste durante un'indagine interna. Una simile reazione all'interno dell'azienda distrugge alla radice la fiducia nei canali di segnalazione. Se una dipendente percepisce che, segnalando una molestia, verrà a sua volta messa sotto esame e colpevolizzata, non si farà mai avanti, creando una cultura dell'impunità. L'unico antidoto è un'azione culturale e formativa proattiva e intransigente, che affermi il principio assoluto secondo cui **la responsabilità di una molestia ricade sempre e solo su chi la compie.**

Impatti psicosociali nel workplace

La violenza contro un singolo individuo contamina l'intero ambiente di lavoro, generando **disfunzioni organizzative** che vanno ben oltre la vittima diretta.

Stress lavorativo e burnout correlato

La violenza online rappresenta uno stressor cronico, imprevedibile e incontrollabile. Costringe la vittima a un "secondo turno" di autodifesa digitale, portandola a un progressivo esaurimento psicofisico (*burnout*) che causa un crollo della performance, difficoltà di concentrazione e un aumento del rischio di turnover, con costi ingenti per l'azienda.

Isolamento professionale e sociale

La vittima tende a ritirarsi per protezione, mentre i colleghi possono allontanarsi per imbarazzo, paura di essere associati o pregiudizio. Questo isolamento, **amplificato nel lavoro da remoto**, priva la persona colpita del flusso di informazioni informali paralizzando la sua capacità di collaborazione e di crescita professionale.

Interferenza con performance e produttività

Il trauma e l'iper-vigilanza impongono un enorme carico cognitivo sulla vittima, limitando la capacità di svolgere il cosiddetto "lavoro profondo" che richiede concentrazione, creatività e problem solving. I manager devono essere formati a riconoscere segnali come errori, calo di motivazione o ritardi non come semplici fallimenti professionali, ma come possibili indicatori di disagio psicologico.

Trauma secondario nei colleghi testimoni

Assistere o venire a conoscenza di episodi di violenza, anche se online, può traumatizzare i colleghi, generando sentimenti di impotenza, rabbia e paura. **Questo fenomeno di trauma vicario erode la coesione del team e la fiducia reciproca.** È fondamentale formare i dipendenti a diventare "*bystander* attivi", trasformando l'impotenza in responsabilità condivisa per un impegno collettivo.

Parte III
Violenza di genere online nel contesto lavorativo

Dopo aver inquadrato i fenomeni della violenza di genere online nella loro dimensione generale, è ora imperativo calare questa analisi all'interno del perimetro aziendale. **Il luogo di lavoro, sia esso fisico o digitale, non è una bolla impermeabile alle dinamiche della società, ma ne è, al contrario, uno specchio.**

La violenza di genere online non si ferma sulla soglia dell'ufficio o alla schermata di login del portale aziendale; la permea, la influenza e la danneggia in modi specifici e misurabili. Comprendere come questa violenza si manifesti "sul lavoro" è un passo cruciale per poterla **prevenire, gestire e sradicare**, proteggendo le persone e, con esse, il valore, la produttività e l'integrità dell'intera organizzazione.

Mappatura dei casi ricorrenti

Per agire efficacemente, bisogna prima di tutto saper riconoscere. **La violenza di genere online nel contesto professionale non è un concetto astratto**, ma si concretizza in una serie di comportamenti e attacchi ricorrenti. Di seguito, una mappatura dettagliata di questi casi, che ogni manager, responsabile HR e dipendente dovrebbe conoscere.

Workplace harassment digitale: molestie via e-mail, chat aziendali, videoconferenze e condivisione non consensuale di contenuti

Con l'espressione "***workplace harassment* digitale**" ci si riferisce a tutte quelle forme di molestia che utilizzano gli strumenti di comunicazione forniti dall'azienda per perpetrare un abuso. In questo caso, la responsabilità dell'organizzazione è diretta e ineludibile, poiché la violenza si consuma all'interno dell'ambiente di lavoro digitale che essa stessa ha creato e che ha il dovere di mantenere sicuro.

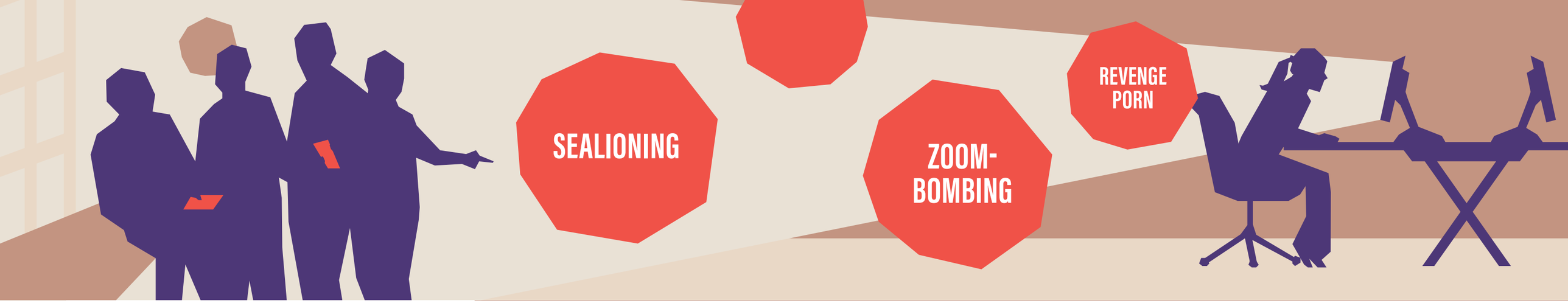
Il vettore più tradizionale, ma ancora estremamente diffuso, è quello delle molestie via e-mail. Questa forma di abuso può essere subdola, poiché spesso non si tratta di minacce esplicite, ma di una "violenza a bassa intensità" che logora la vittima nel tempo. Può manifestarsi con l'invio sistematico di battute a sfondo sessista, commenti non richiesti sull'aspetto fisico, la condivisione di link a contenuti inappropriati, o l'uso di un tono costantemente aggressivo e svilente.

Le chat aziendali, come Slack, Microsoft Teams o altre piattaforme di messaggistica istantanea, rappresentano un'altra frontiera di rischio. La loro natura semi-informale può abbassare le inibizioni e favorire la nascita di dinamiche tossiche. Le molestie in questo contesto possono assumere forme diverse: l'esclusione deliberata e sistematica di una collega da un gruppo di lavoro cruciale per un progetto; l'invio di messaggi privati a sfondo sessuale o con richieste inopportune; l'uso di emoji, meme o GIF per veicolare messaggi sessisti o denigratori; o, ancora, la creazione di canali "ombra" in cui un gruppo di colleghi si accorda per isolare o deridere una persona.

L'avvento massiccio del lavoro da remoto ha aperto un ulteriore canale di vulnerabilità: le videoconferenze. Durante una riunione online, la molestia può avvenire in modo palese o nascosto. Può trattarsi di commenti inappropriati sull'aspetto fisico della persona o sul suo ambiente domestico visibile in camera; dell'invio di messaggi molesti tramite la funzione di chat privata durante una riunione di gruppo; o dell'uso della funzione di condivisione dello schermo per mostrare, magari con la scusa di un errore, contenuti offensivi o pornografici.

A queste dinamiche si aggiunge **la condivisione non consensuale di contenuti in ambito professionale.** È fondamentale capire che non si tratta solo della diffusione di immagini intime, ma di una violazione della privacy digitale che può avvenire con contenuti di natura diversa. Un esempio comune è lo screenshot di una conversazione privata o di un post personale di una collega sui suoi social media, che viene poi condiviso in una chat di lavoro con lo scopo di deriderla, criticarla o metterla in cattiva luce con i superiori.

Queste pratiche sortiscono l'effetto di erodere la **sicurezza psicologica** della vittima, fondamentale per la salute e la performatività del team di cui è parte.



Quando le persone hanno paura che le loro parole possano essere decontestualizzate e usate contro di loro, smettono di esprimere opinioni, di proporre idee e di fidarsi dei colleghi. **Si crea un clima di sospetto e di ansia che inibisce la collaborazione e la creatività.**

Poiché il molestatore può sempre nascondersi dietro la scusa dello "scherzo", del "complimento" o del "fraintendimento", la sfida per le aziende è monitorare e agire efficacemente nella "zona grigia" in cui molti di questi comportamenti si collocano. È proprio per questo che **le policy aziendali devono essere estremamente chiare e specifiche nel definire quali sono i comportamenti digitali inaccettabili**, e la formazione deve fornire a tutti gli strumenti per riconoscerli e segnalarli, senza timore di ritorsioni.

Professional reputational attack: campagne diffamatorie e gender-based trolling su piattaforme professionali

Questa seconda categoria di attacchi si distingue per avere un obiettivo mirato e strategico: non solo ferire la persona, ma **distruggere la sua credibilità, la sua competenza e la sua reputazione professionale.** Sono armi utilizzate per sabotare le carriere, specialmente quelle di donne che raggiungono posizioni di vertice o di alta visibilità.

Le campagne diffamatorie sono spesso sistematiche: possono includere la diffusione di false voci sull'incompetenza di una professionista via e-mail o social media, la scrittura di recensioni false e denigratorie su siti professionali, o la creazione di interi siti web o blog dedicati a screditare il suo lavoro.
Gli autori di queste campagne possono essere diversi: un concorrente, un ex dipendente scontento, un ex partner che cerca di rovinarla finanziariamente, o persino un collega interno in competizione per la stessa promozione.

Un terreno di scontro sempre più comune sono **i profili social che si prestano a fornire un bersaglio privilegiato per il trolling di genere.** Le professioniste che li utilizzano per condividere le proprie competenze, pubblicare articoli o celebrare un successo lavorativo vengono sistematicamente prese di mira.

Le tattiche utilizzate su queste piattaforme mirano a minare l'autorevolezza della vittima di fronte alla sua rete professionale. Includono commenti che ne mettono in dubbio le credenziali, che la inondano di **domande pretestuose per mandare la discussione fuori tema** (***sealioning***), o che ricorrono a stereotipi sessisti per sminuirne i risultati.

Le conseguenze di questi **attacchi reputazionali** sono tangibili e, in alcuni casi, possono divenire anche **devastanti.**

Una reputazione professionale danneggiata può tradursi **nella perdita di clienti, nella difficoltà a trovare nuove opportunità lavorative, o nell'essere scavalcata in una promozione.** Per l'azienda inoltre, un attacco mirato a una sua figura chiave può causare **un danno d'immagine, minare la fiducia degli investitori e mettere in discussione la sua capacità di proteggere i propri talenti.**
Il ruolo dell'azienda di fronte a questi attacchi è delicato ma **cruciale**: sebbene non possa controllare l'intera rete internet, non può rimanere passiva. Ignorare un attacco reputazionale contro una propria dipendente equivale a comunicare, internamente ed esternamente, che l'azienda non difende il proprio capitale umano.

Smart working e nuove vulnerabilità: *zoom-bombing* e *revenge porn* tra colleghi

Lo smart working, se da un lato ha offerto flessibilità, ha dall'altro demolito le barriere fisiche che un tempo separavano l'ambiente di lavoro dalla vita privata, creando **un nuovo e complesso panorama di rischi.**

Questa nuova "intimità digitale" ha generato **vulnerabilità inedite** che le aziende devono imparare a gestire.

Un fenomeno emblematico è lo "***zoom-bombing***". Con questo termine si indica **l'intrusione dolosa e non autorizzata di una o più persone all'interno di una riunione in videoconferenza**, con lo scopo di sabotarla, spesso attraverso la condivisione di contenuti scioccanti, pornografici o violenti.

È fondamentale sottolineare che **questi attacchi hanno spesso una chiara matrice di genere e non sono casuali.** Vengono deliberatamente indirizzati a riunioni organizzate da donne o a webinar su temi come la parità di genere. Lo "*zoom-bombing*" diventa così un attacco politico, un'azione violenta volta a negare alle donne il diritto di riunirsi e di parlare in uno spazio pubblico, anche se virtuale.

La responsabilità di prevenire questi attacchi ricade interamente sull'azienda che organizza la riunione. È infatti l'azienda che deve garantire la sicurezza delle proprie "sale riunioni virtuali". Questo richiede l'adozione di misure tecniche basilari (come l'uso di password, l'attivazione delle "sale d'attesa", l'obbligo di autenticazione per i partecipanti) e la definizione di protocolli di risposta chiari.

Infine, il contesto del lavoro da remoto ha acuito un rischio estremamente sensibile: **il *revenge porn* che coinvolge colleghi o superiori.**
La maggiore informalità e la distanza fisica possono talvolta favorire la nascita di relazioni intime tra persone che lavorano insieme.
Quando queste relazioni finiscono, o quando si basano su uno squilibrio di potere, il materiale intimo scambiato consensualmente può

essere trasformato in un'arma di ricatto o di vendetta all'interno della stessa azienda.

Questa dinamica rappresenta **una sfida immensa per le funzioni HR e Compliance**. La vittima, infatti, si trova di fronte a un dilemma terribile: denunciare l'accaduto, col rischio di non essere creduta e di subire ritorsioni professionali, o cedere al ricatto. Per questo motivo, **è vitale che le aziende dispongano di canali di segnalazione (*whistleblowing*) estremamente sicuri e indipendenti**, che possano garantire alla vittima la massima riservatezza.

Impatti sulla carriera professionale

La violenza di genere online non è un evento che si esaurisce nello spazio privato dello schermo, ma si propaga con forza devastante nella vita professionale delle vittime, minandone le fondamenta economiche, limitandone la visibilità e costruendo nuove e insidiose barriere alla loro crescita.
L'impatto della violenza digitale sulla carriera non è un "danno collaterale", ma spesso lo scopo primario dell'attacco. L'obiettivo dell'aggressore è frequentemente quello di colpire la vittima nella sua dimensione pubblica e professionale, perché è lì che si manifesta la sua autonomia e competenza.

Conseguenze economiche e professionali

La violenza di genere online rappresenta anche una sfida economica. Essa impone costi finanziari, diretti e indiretti, che possono compromettere gravemente la stabilità economica della vittima.

I **costi diretti** sono le spese immediate che la vittima è costretta a sostenere per difendersi. **Spesso deve rivolgersi a un legale per inviare diffide o presentare querele.** A questi si aggiungono i costi per un supporto psicologico, essenziale per elaborare il trauma. In molti casi, le vittime sono inoltre costrette ad avvalersi di servizi specializzati in reputation management online, operazioni complesse e molto costose.

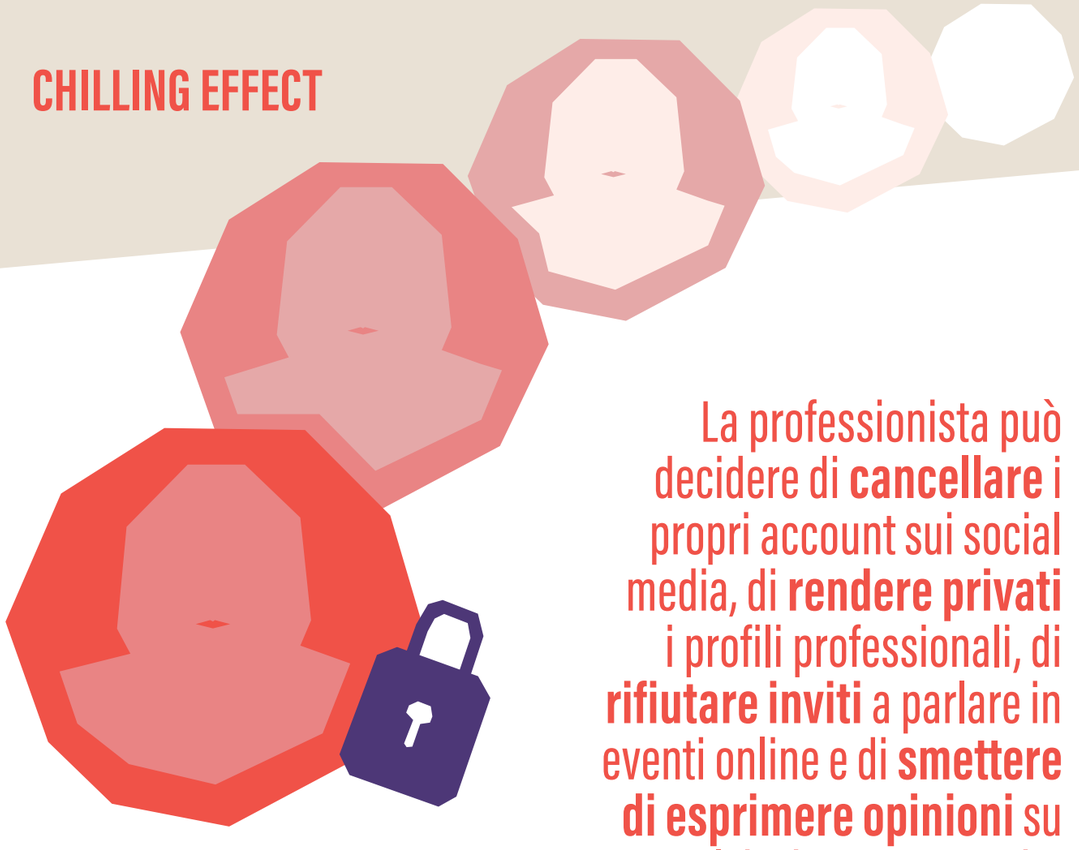
I **costi indiretti** sono ancora più pesanti e si manifestano attraverso la perdita di produttività sul lavoro. È umanamente impossibile per una persona che sta subendo un attacco digitale costante mantenere lo stesso livello di concentrazione. Questo si traduce in un calo misurabile della performance, che può portare a valutazioni negative, alla mancata assegnazione di bonus o di aumenti salariali, e a un rallentamento del percorso di carriera.

A questo si aggiunge **la perdita di opportunità lavorative concrete.** Oggi, è prassi comune per qualsiasi recruiter o potenziale cliente effettuare una ricerca online sul nome di un candidato. Se la candidata non ha la libertà di esprimersi a causa degli attacchi che riceve o sa di ricevere, la sua presenza online sarà certamente meno efficace rispetto a quella di chi invece non ha alcun timore.

L'impatto è particolarmente catastrofico per le lavoratrici autonome, le consulenti e le imprenditrici, la cui **reputazione online** rappresenta il loro principale asset commerciale.

Infine, **lo stress e il trauma possono costringere la vittima a un lungo periodo di assenteismo** per malattia o, nei casi più gravi, a dimettersi dal proprio posto di lavoro, con la conseguente perdita totale del proprio reddito. Il ruolo dell'azienda nel mitigare questi danni è fondamentale, attraverso policy che prevedano supporto legale, psicologico e permessi retribuiti speciali.

CHILLING EFFECT



La professionista può decidere di **cancellare** i propri account sui social media, di **rendere privati** i profili professionali, di **rifiutare inviti** a parlare in eventi online e di **smettere di esprimere opinioni** su qualsiasi argomento che possa essere percepito come "**controverso**".

Autocensura e limitazione della presenza online

Forse la conseguenza più subdola della violenza di genere online è **l'autocensura**, anche denominata "***chilling effect***" (effetto raggelante) che consiste nella decisione, spesso non del tutto cosciente, di **ritirarsi dal dibattito pubblico digitale e di limitare la propria espressione** per paura di diventare un bersaglio.

Possiamo pensare alla presenza online di una professionista come a un suo asset strategico, come si è detto pocanzi in relazione alla potenziale ricerca da parte di un recruiter. L'ambiente digitale oggi rappresenta per tutti uno spazio in cui costruire o coltivare la propria rete di contatti e dimostrare la propria competenza. L'autocensura, in questa analogia, equivale a essere **costretta a non uscire** più di casa per timore di essere aggredita.

Questa ritirata si manifesta in comportamenti concreti e osservabili.

Ritirandosi, la professionista subisce **una drastica perdita di "capitale sociale" e di visibilità**: la rete di contatti smette di crescere con il rischio di diventare progressivamente invisibile ai recruiter, head-hunter e potenziali clienti. L'impatto sulla crescita professionale a lungo termine è incalcolabile, poiché le posizioni di vertice vengono sempre più spesso affidate a persone che hanno saputo costruire un personal brand forte.

Questo fenomeno non danneggia solo la singola professionista, ma rappresenta un'enorme perdita anche per l'azienda. Quando una dipendente di talento si auto-censura, l'organizzazione perde una potenziale ambasciatrice del proprio brand. È uno spreco di capitale umano e intellettuale che nessuna azienda competitiva può permettersi.

Glass ceiling digitale

La somma di tutte queste conseguenze dà vita a una barriera nuova e invisibile: il **"soffitto di cristallo digitale"** (**c.d. *digital glass ceiling*).** Si tratta di un ostacolo alla carriera delle donne, interamente costruito nello spazio online, che impedisce o rallenta drasticamente la loro ascesa verso posizioni di leadership.

Questo soffitto si costruisce "mattone su mattone". È il risultato del carico mentale aggiuntivo che le donne devono sopportare per gestire un ambiente lavorativo ostile traslato online, delle opportunità professionali perse a causa di una reputazione danneggiata e della perdita di visibilità dovuta all'autocensura.

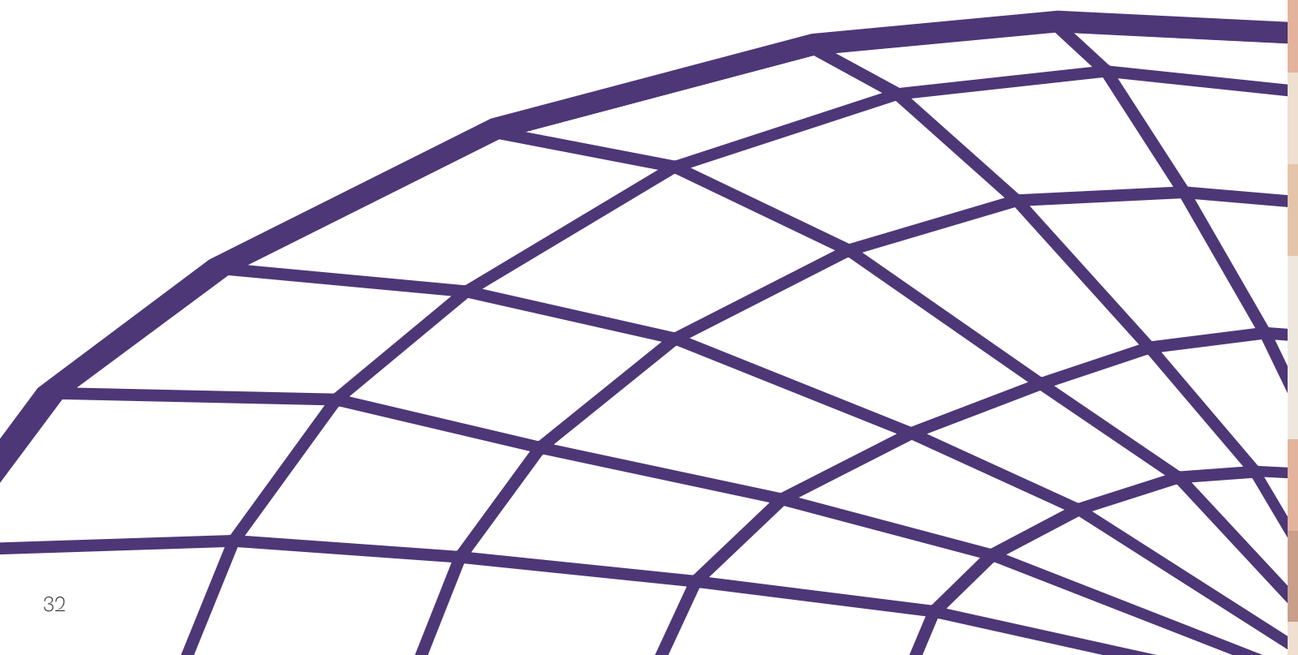
Un elemento cruciale nella costruzione di questa barriera è il **bias inconscio nella valutazione** da parte del management.

Capita spesso che una leader donna che si trova al centro di una campagna d'odio online, invece di essere vista come la vittima, può essere percepita come **una figura "divisiva" o "problematica"**: anziché ricevere supporto, viene etichettata come un rischio per la reputazione aziendale, con un impatto nefasto sulle sue possibilità di promozione.

A questo si aggiunge un **doppio standard** di comportamento online.

Mentre ai leader uomini è spesso concessa una comunicazione più diretta, **dalle leader donne ci si aspetta un comportamento digitale impeccabile e mai controverso.** Il semplice fatto di diventare bersaglio di attacchi (anche senza colpa) viene giudicato molto più severamente.

L'effetto di questa barriera è sistemico e demotiva tutte le donne ambiziose all'interno dell'organizzazione. Esse osservano e imparano che avere una voce forte e una presenza pubblica visibile - qualità oggi considerate essenziali per la leadership - le espone a un rischio enorme che può essere usato contro di loro anche internamente. Ciò le dissuade dal perseguire percorsi di carriera di vertice, impoverendo la pipeline di leadership dell'azienda.



Parte IV
Strategie di contrasto aziendali

La consapevolezza del problema, per quanto essenziale, non è sufficiente. Per tradurre l'intenzione in interventi concreti capaci di portare un cambiamento profondo, **è necessario un piano d'azione strategico, strutturato e integrato in tutti i processi aziendali.** La lotta alla violenza di genere online non può essere delegata a iniziative sporadiche o a campagne di comunicazione estemporanee; **deve diventare una componente fondamentale della governance, della cultura e della gestione del rischio dell'organizzazione.**

Questa sezione è concepita come un vero e proprio manuale operativo che fornisca una roadmap chiara per guidare le aziende in un percorso di trasformazione da una posizione reattiva - in cui si interviene, spesso in modo disorganizzato, solo dopo che un incidente si è verificato - a **una posizione proattiva e resiliente, in cui si prevengono gli abusi, si proteggono le persone e si promuove una cultura digitale sicura.**

Assesment e mappatura dei rischi

Il primo, ineludibile passo di qualsiasi strategia efficace è **la diagnosi.** Nessuna azienda può proteggersi da un rischio che non comprende o di cui sottovaluta la portata. Così come si conducono audit sulla sicurezza informatica o valutazioni sul rischio di incendio, è oggi imperativo condurre un'analisi rigorosa dei rischi specifici legati alla violenza di genere online.

Questo processo è **un momento di fondamentale autocoscienza organizzativa.** Non esiste una soluzione valida per tutti; l'obiettivo è creare una "fotografia" su misura del profilo di rischio della propria organizzazione, per poter poi disegnare interventi mirati e realmente efficaci.

Risk assesment framework per la violenza di genere online

Per condurre l'analisi in modo sistematico, è necessario adottare una metodologia strutturata che guidi l'azienda nell'identificazione, analisi e valutazione dei rischi. Un framework efficace per la violenza di genere online si articola in **quattro passaggi fondamentali.**

L'identificazione dei pericoli

I "pericoli" sono le diverse forme di violenza che abbiamo descritto: **l'hate speech, l'IBSA, il cyberstalking, il doxxing.** Il team incaricato dell'assesment deve dunque porsi la domanda: "Considerando la natura del nostro business e la nostra cultura, quali di queste forme di violenza hanno la maggiore probabilità di manifestarsi?".

Identificare chi è a rischio e come

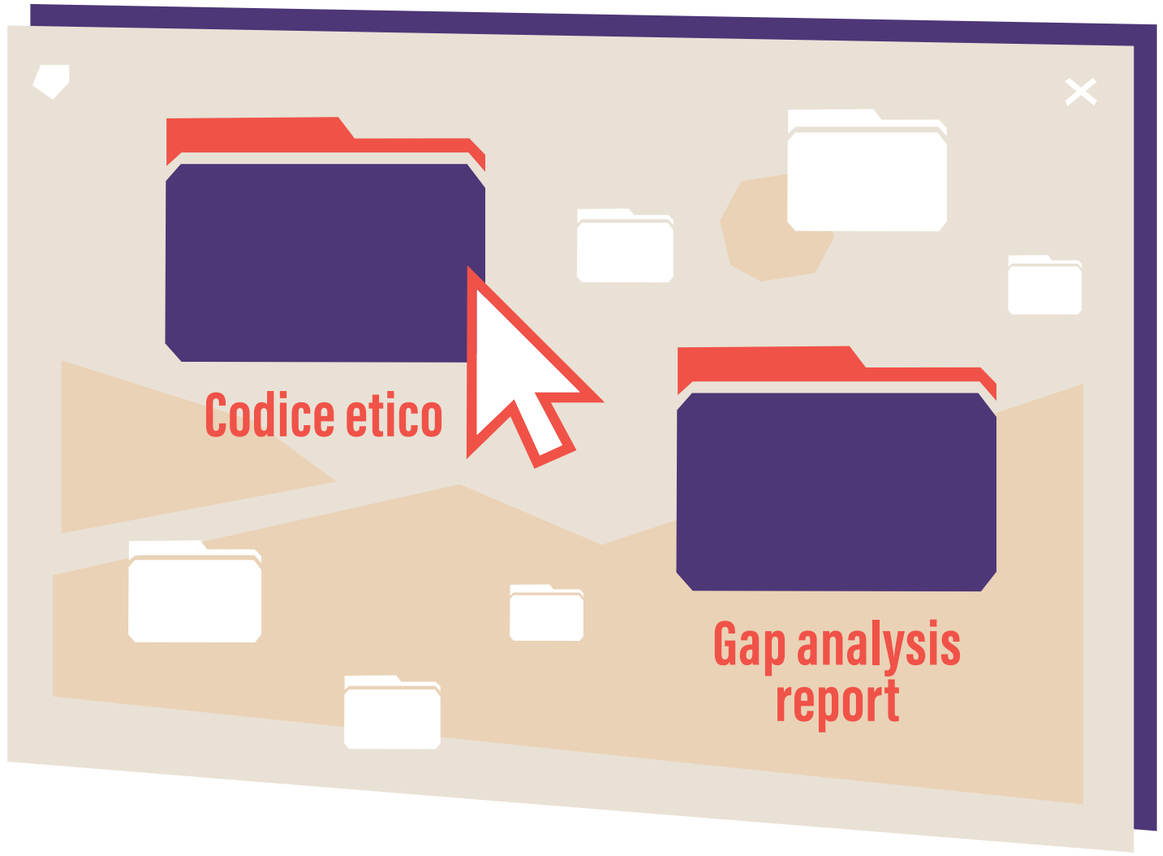
Questo richiede **una mappatura dei ruoli e delle persone più esposte** all'interno dell'organizzazione: figure apicali, dipendenti a contatto con il pubblico, donne in settori a predominanza maschile.

La valutazione del rischio e dei controlli

Per ogni rischio, l'azienda deve valutarne la probabilità e il potenziale impatto. Successivamente, è necessario analizzare con onestà quali **misure di controllo** sono già operative per mitigare quel rischio.

La registrazione dei risultati e la creazione di un piano d'azione

L'analisi deve essere formalizzata in **un documento che riassuma i rischi principali, ordinandoli per priorità.** Per ogni rischio ad alta priorità, deve essere definito un piano di miglioramento concreto. È fondamentale che questo documento di valutazione del rischio sia **un documento vivo**, da rivedere e aggiornare con cadenza periodica.



Audit delle policy esistenti

Parallelamente alla valutazione dei rischi, è indispensabile condurre **un audit critico di tutte le policy aziendali pertinenti** per verificare se l'infrastruttura normativa interna sia sufficientemente robusta o se presenti lacune.

Il punto di partenza è il Codice Etico o di Condotta dell'azienda, che deve menzionare esplicitamente la tolleranza zero verso ogni forma di molestia, incluse quelle online.

Successivamente, l'analisi deve concentrarsi sulla **policy anti-molestie**, che deve essere aggiornata per includere una definizione chiara e dettagliata di molestia digitale, fornendo esempi concreti.

Un altro documento chiave è **la policy sull'uso degli strumenti informatici**, che deve proibire esplicitamente l'utilizzo di qualsiasi risorsa aziendale per porre in essere comportamenti molesti. Con la normalizzazione del lavoro da remoto, è diventato essenziale esaminare anche **la policy sullo smart working**, che deve includere un capitolo dedicato all'etichetta e alla condotta professionale nell'ambiente di lavoro digitale.

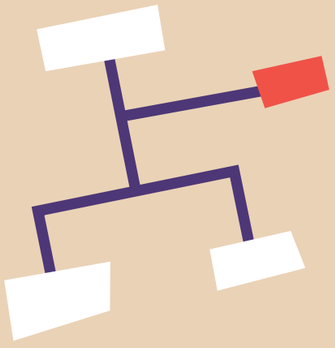
L'esito di questo audit dovrebbe essere un "***gap analysis report***": un documento che evidenzia con precisione le lacune e le aree di debolezza delle policy attuali. Le policy, inoltre, non devono essere documenti isolati, ma **integrate e coerenti** tra loro. Infine, l'audit non può limitarsi all'analisi dei testi, ma deve valutare anche i processi di comunicazione, formazione e applicazione (*enforcement*).

Identificazione delle vulnerabilità tecnologiche e organizzative

L'ultimo pilastro della fase di assessment è **l'identificazione delle vulnerabilità**, ovvero di quei punti deboli, di natura tecnologica, procedurale o culturale, che un aggressore potrebbe sfruttare per infliggere un danno.

Le vulnerabilità tecnologiche

Riguardano **l'infrastruttura digitale**: la configurazione dei sistemi di chat aziendale, la sicurezza delle piattaforme di videoconferenza, la robustezza della moderazione dei commenti sui canali social aziendali, o l'involontaria esposizione di dati personali dei dipendenti sul sito web corporate.



Le vulnerabilità organizzative

Sono spesso le più difficili da individuare, ma ancora più pericolose. La prima e più critica riguarda **i canali di segnalazione**: sono sicuri, accessibili e garantiscono la confidenzialità? Esiste un canale di whistleblowing anonimo?
Un'altra grave vulnerabilità organizzativa è la mancanza di una formazione adeguata. La formazione su questi temi è obbligatoria per tutti, inclusi i dirigenti? È un evento sporadico o un processo continuo e interattivo?

Le vulnerabilità culturali

La vulnerabilità **più profonda e pervasiva.** Esiste in azienda una cultura che tollera le battute sessiste? La leadership è la prima a modellare un comportamento inclusivo e rispettoso? L'obiettivo finale di questo processo è la creazione di una "**mappa delle vulnerabilità**", che fornisce la più potente e lucida chiamata all'azione.

Roadmap implementativa

Questo percorso strutturato in **quattro fasi** guida l'azienda nel processo di cambiamento.

Fase 01 — Analisi e mappatura degli stakeholder (Mesi 1-3)

Formalizzare l'assessment in un business case e costruire una coalizione interna, creando un gruppo di lavoro interfunzionale con un mandato chiaro dal vertice.

Fase 02 — Sviluppo di policy e procedure (Mesi 4-9)

Sviluppare o aggiornare le policy, creando procedure operative chiare per la segnalazione (*whistleblowing*), l'investigazione e il supporto alla vittima.

Fase 03 — Implementazione e formazione aziendale (Mesi 10-18)

Lanciare nuove policy con una campagna di comunicazione, erogare la formazione a tutti i livelli (base, manager, *bystander*) e implementare le soluzioni tecnologiche.

Fase 04 — Monitoraggio continuativo e miglioramento

Definire e monitorare un cruscotto di KPI, produrre report periodici per il management e usare i dati per avviare un ciclo di miglioramento continuo.

Policy e Governance

Le strategie devono essere incardinate nella struttura di governo e controllo dell'azienda per garantirne **la sostenibilità e l'efficacia.**

Integrazione nei Modelli 231 e Compliance

Integrare la prevenzione della violenza online nel **Modello di Organizzazione e Gestione** (ove applicabile) eleva il tema a rischio penale-amministrativo per l'ente, conferendo all'**Organismo di Vigilanza** un mandato di controllo e rafforzando il sistema di compliance generale. D'altronde come si è detto, non è da escludere che in un prossimo futuro alcuni reati digitali come il deepfake vengano inclusi nel c.d. catalogo dei reati 231, da cui può discendere la responsabilità amministrativa dell'ente.

Codici Etici e di condotta digitale

Il Codice Etico deve **condannare esplicitamente la violenza online.** Un Codice di Condotta Digitale specifico invece dovrebbe avere l'obiettivo di tradurre i valori in regole di comportamento chiare per gli spazi digitali interni ed esterni, collegando il loro rispetto ai sistemi di valutazione della performance. Distinguere i due codici potrebbe essere estremamente significativo per invitare il personale ad una attenta riflessione sulle **conseguenze reali** delle azioni digitali che attuiamo ogni giorno.

Whistleblowing e canali di segnalazione sicuri

È fondamentale implementare **un sistema di segnalazione multicanale**, che includa una piattaforma di *whistleblowing* sicura, confidenziale e preferibilmente gestita da terzi, con una politica a tolleranza zero verso ogni forma di ritorsione in conseguenza della denuncia stessa.

Protocolli di gestione crisi reputazionali

L'azienda deve avere **un protocollo predefinito** per gestire lo scenario in cui un incidente diventi di dominio pubblico, con un team di crisi designato e principi di comunicazione basati su velocità, trasparenza ed empatia.

Formazione e educazione digitale

La formazione è lo strumento principale per **tradurre le policy in comportamenti agiti** e porle a fondamento di una cultura aziendale condivisa.

Digital literacy

Un programma di **alfabetizzazione digitale di base**, obbligatorio e continuo, che copra la comprensione dei fenomeni, la conoscenza delle policy aziendali e la sicurezza digitale personale.

Bystander training

Formazione pratica e basata su scenari reali per **trasformare i testimoni passivi in alleati attivi**, fornendo un ventaglio di strategie di intervento sicure ed efficaci.

Leadership training

Formazione avanzata per i manager su come **riconoscere i segnali di disagio e gestire la prima risposta** a una confidenza in modo empatico e corretto.

Victim support

Formazione specialistica per le funzioni HR e di supporto, **basata su un approccio trauma-informed**, per garantire una gestione del caso che sia compassionevole e non riproduca il trauma. In particolare, l'obiettivo è quello di **evitare o prevenire ove possibile le conseguenze del *victim blaming*** e della vittimizzazione secondaria.

L'importanza del consenso e le soluzioni tecnologiche

Uno strumento importante, se non fondamentale, che deve essere compreso per un corretto utilizzo delle risorse digitali è **il consenso.** Il consenso rappresenta lo strumento giuridico fondamentale, attraverso cui l'utente acquisisce piena consapevolezza delle implicazioni e delle conseguenze derivanti dal conferimento dei propri dati personali negli ecosistemi digitali contemporanei. Tale meccanismo costituisce **il presupposto legittimante imprescindibile per qualsiasi forma di trattamento di informazioni personali**, incluse immagini, contenuti multimediali e tracce digitali, configurandosi come barriera normativa essenziale contro le violazioni sistematiche dei cosiddetti nuovi diritti fondamentali digitali. Ogni utilizzo dell'immagine o di qualsiasi categoria di dati riferibili a una persona fisica risulta consentito esclusivamente attraverso l'acquisizione del consenso valido della stessa.

L'ambiente digitale contemporaneo genera quotidianamente **una produzione massiva e ininterrotta di tracce informative** da parte degli utenti, i quali aderiscono sistematicamente a servizi e piattaforme digitali mediante l'accettazione automatica e acritica di complessi termini contrattuali e articolate informative sul trattamento dei dati personali, senza procedere alla loro lettura e comprensione.

Questo processo meccanicizzato e standardizzato comporta **una sostanziale e preoccupante disconnessione tra l'atto formale dell'assenso e la comprensione materiale e consapevole delle sue implicazioni e conseguenze giuridiche a lungo termine.** L'analisi consapevole e approfondita della documentazione contrattuale, unitamente alla valutazione critica e ponderata degli impegni assunti e delle responsabilità derivanti, costituiscono **gli strumenti di tutela e protezione più efficaci** attualmente a disposizione dell'utente, benché sistematicamente e inspiegabilmente disattesi dalla maggioranza degli utilizzatori.

Il paradigma digitale contemporaneo presenta un evidente e preoccupante **paradosso strutturale di natura sistemica**: mentre il consenso formalmente sottende e legittima ogni singola interazione telematica - dalla registrazione iniziale ai servizi fino alla condivisione quotidiana di contenuti personali e altrui - la sua percezione effettiva da parte degli utenti rimane sostanzialmente confinata a mero adempimento formale e burocratico, completamente privo di significato sostanziale e di comprensione reale.

La riduzione dell'assenso consapevole a semplice **"click" meccanico e automatico** trasforma quello che dovrebbe essere un atto fondamentale di autodeterminazione informativa in una mera routine, vanificando completamente la funzione protettiva e garantista che il consenso dovrebbe svolgere per definizione, con la conseguenza che anche la violazione del consenso non viene percepita come un illecito.

L'implementazione diffusa e consapevole di una cultura del consenso digitale realmente informato e partecipato genererebbe necessariamente **effetti deterrenti significativi e misurabili** contro le numerose condotte lesive perpetrate quotidianamente negli ambienti online.

La piena comprensione collettiva che la condivisione non autorizzata di contenuti, immagini e informazioni riferibili ad altri soggetti costituisce una violazione della dignità personale sostanzialmente equiparabile a quella fisica per gravità e conseguenze, unitamente alla diffusa consapevolezza che l'esercizio legittimo della propria libertà di espressione trova necessariamente il proprio limite invalicabile nel **diritto fondamentale altrui al controllo della propria immagine**, reputazione e privacy, costituirebbe il solido fondamento etico e giuridico di un ecosistema digitale interamente basato sui principi del consenso affermativo, consapevole e non meramente presunto.

Tale innovativo approccio culturale richiede necessariamente **il pieno riconoscimento che il consenso digitale possiede identica valenza normativa, etica e responsabilità rispetto a quello richiesto nelle interazioni fisiche** per quanto concerne il rispetto dell'intimità, della dignità e dell'autodeterminazione personale.

Per affrontare efficacemente l'odio online, le molestie virtuali e la maggior parte degli illeciti già descritti, sono necessari **approcci interdisciplinari, ovvero un'azione coordinata tra privato e pubblico in grado di creare comunità di utenti consapevoli**, attraverso una costante riflessione etica in particolare riferita alla cosiddetta cultura del consenso, che è diventato centrale quando si parla di violenza di genere. Questa importante opera di sensibilizzazione e educazione digitale deve essere supportata da **strumenti e processi robusti** che rendano la sicurezza un elemento intrinseco dell'ambiente di lavoro digitale.

Strumenti di monitoring e early detection

Utilizzo etico e conforme alla legge di strumenti tecnologici per **il monitoraggio proattivo delle piattaforme interne ed esterne**, al fine di identificare rischi e attacchi in fase iniziale.

Configurazioni privacy e sicurezza avanzate

Implementazione del principio di "**Security by Design**" per rafforzare la sicurezza delle piattaforme e audit dei canali pubblici per minimizzare l'esposizione di dati personali dei dipendenti.

Protocolli di incident response

Avere **un "manuale operativo" predefinito e testato tramite simulazioni**, che delinei i passaggi da seguire in caso di incidente: triage, attivazione del team, investigazione e supporto alla vittima.

Protocolli di incident response

Costruire relazioni proattive con **i team di *trust & safety*** delle principali piattaforme social o di associazioni e ONG che lavorano con le piattaforme per **accelerare le procedure di rimozione (*takedown*) di contenuti lesivi.**

Parte V
Best practice internazionali

Le buone pratiche, quando documentate e verificabili, offrono un riferimento concreto per passare dalla teoria all'azione. Analizzare casi reali permette di individuare soluzioni efficaci, misurarne i risultati e capire quali elementi possano essere replicati nel proprio contesto. In questa sezione vengono presentate **esperienze internazionali** che dimostrano come sia possibile sviluppare strategie di impatto misurabile.

Best practice internazionali

Le organizzazioni internazionali più innovative hanno sviluppato **approcci multidimensionali e integrati per affrontare in maniera strutturale le problematiche legate a molestie**, discriminazioni e comportamenti non inclusivi. Questi approcci si articolano lungo diverse direttrici complementari, che interagiscono tra loro per generare un cambiamento sistemico:

Policy-driven approach

Molte istituzioni hanno compreso l'importanza di adottare **un quadro normativo chiaro e vincolante**, costruendo politiche interne specifiche contro le molestie e le discriminazioni. Queste policy definiscono procedure dettagliate per la segnalazione, la gestione dei reclami e la protezione delle vittime e dei testimoni. In diversi casi, vengono anche introdotti **codici di condotta aggiornati, linee guida operative e regolamenti interni** che sanciscono esplicitamente le conseguenze disciplinari in caso di violazioni, per una maggiore trasparenza e tutela.

Technology-enabled solutions

Parallelamente, la tecnologia viene utilizzata come **leva strategica** per rafforzare i processi di prevenzione e risposta. Tra gli strumenti più diffusi figurano piattaforme digitali sicure e anonime per le segnalazioni, sistemi di monitoraggio dei dati per individuare pattern ricorrenti di rischio, e applicazioni mobili dedicate al **supporto immediato** delle persone coinvolte.

Alcune organizzazioni hanno introdotto anche strumenti basati sull'intelligenza artificiale per analizzare linguaggi e dinamiche interne.

Culture transformation

La sola adozione di regole e strumenti non è sufficiente senza **un profondo cambiamento della cultura organizzativa.** Per questo, le organizzazioni internazionali più avanzate investono in programmi di formazione continua e leadership inclusiva. L'obiettivo è quello di costruire **un ambiente lavorativo basato sul rispetto reciproco**, al fine di creare spazi sicuri in cui ogni persona possa esprimersi senza timore. Le iniziative culturali possono includere campagne di comunicazione interna, workshop interattivi, percorsi di mentoring e momenti di confronto che favoriscono la consapevolezza collettiva.

Accountability systems

Infine, un elemento fondamentale è rappresentato dai **meccanismi di monitoraggio e responsabilizzazione.** Le organizzazioni più innovative implementano sistemi strutturati di raccolta dati, report periodici e audit indipendenti che misurano l'efficacia delle politiche e delle iniziative intraprese. Ciò consente di garantire trasparenza e individuare eventuali aree di miglioramento.

Case Study

Salesforce – “Equality for All” program

Salesforce, leader mondiale nel settore del crm cloud-based, si è trovata a partire dal 2015 di fronte a importanti sfide in materia di diversità, equità e inclusione, in particolare nel contrasto alle molestie e alle discriminazioni nel contesto del digital workplace. L’azienda ha riconosciuto come i dati di settore fossero allarmanti: **circa il 73% delle donne impiegate nel comparto tecnologico aveva dichiarato di aver subito almeno una forma di discriminazione o molestia online in ambito lavorativo.** Tale evidenza ha spinto Salesforce a **ripensare in modo radicale le proprie politiche interne**, con l’obiettivo di costruire una cultura organizzativa fondata sull’inclusione, sulla trasparenza e sulla sicurezza psicologica dei propri dipendenti.

Strategia implementata: “Equality for All”
Il programma “Equality for All” si articola su tre assi principali - **A) policy, B) tecnologia e C) formazione** - ed è stato concepito per affrontare in maniera integrata i rischi legati a molestie e discriminazioni, nonché per incrementare la rappresentanza dei gruppi sottorappresentati.

A) **Revisione delle policy** e rafforzamento della trasparenza

Nel 2022 Salesforce ha introdotto modifiche sostanziali agli accordi di non divulgazione (nda), consentendo ai dipendenti di poter parlare liberamente di eventuali esperienze di molestie o discriminazioni sul luogo di lavoro. Questa scelta, ispirata a un quadro normativo sviluppato nello stato della California, ha rappresentato un cambio di paradigma volto a rafforzare la fiducia interna e a rompere la cultura del silenzio.

B) Investimenti in **tecnologia anti-harassment**

Salesforce ha investito in soluzioni tecnologiche avanzate per prevenire e gestire episodi di molestie in ambienti digitali e ibridi, grazie a:
a. Sistemi di intelligenza artificiale per il monitoraggio di comportamenti inappropriati nelle comunicazioni aziendali digitali;
b. Chatbot dedicati che permettono segnalazioni anonime e sicure da parte dei dipendenti;
c. Dashboard in tempo reale per i team hr, in grado di tracciare incidenti e rilevare pattern di rischio.

C) **Formazione** e educazione digitale

Parallelamente, l’azienda ha introdotto percorsi formativi obbligatori a tutti i livelli organizzativi, con focus specifici su:
a. Unconscious bias e digital harassment, per accrescere la consapevolezza individuale e collettiva;
b. Bystander intervention training, progettato per contesti di lavoro ibridi e digital-first;
c. Leadership accountability programs, finalizzati a responsabilizzare i manager nel promuovere ambienti inclusivi e sicuri.

Risultati
L’implementazione del programma ha generato progressi significativi, documentati attraverso indicatori quantitativi:

+35% Di **rappresentanza femminile** in posizioni di leadership (2015–2023);

-60% Di **segnalazioni di molestie digitali interne**, evidenziando un impatto tangibile sulla prevenzione;

+28% Nel punteggio relativo alla “**psychological safety**” nelle survey interne di soddisfazione dei dipendenti.

Replicabilità e adattamento
Il modello di Salesforce ha dimostrato di possedere un elevato grado di scalabilità e adattabilità, tanto da essere adottato da oltre 150 aziende tecnologiche a livello globale.
Di seguito, i principali elementi chiave di questa replicabilità.

Standardizzazione dei playbook di implementazione, che offrono **linee guida operative chiare**;

Condivisione di **toolkit tecnologici open-source**, che abbattono barriere di accesso e costi;

Collaborazioni con università e centri di ricerca, a garanzia di un aggiornamento continuo e basato sull’evidenza.

Altri casi di eccellenza internazionale

Microsoft - "Culture reset" initiative
Nel 2018 Microsoft è stata al centro di una delle controversie legali più rilevanti del settore tecnologico in tema di discriminazione di genere. La class action, nota come **Moussouris v. Microsoft**, prendeva il nome dall'ex dipendente Katherine Moussouris e accusava l'azienda di avere alimentato per anni **un ambiente di lavoro segnato da molestie e disparità di trattamento contro le donne impiegate in ruoli tecnici.** Secondo i documenti depositati, tra il 2010 e il 2016 sarebbero state presentate internamente 238 denunce (di cui 108 per molestie sessuali e 119 per discriminazione di genere), ma soltanto una di queste sarebbe stata ritenuta fondata dalle indagini interne. Pur non avendo ottenuto la certificazione della class action per tutte le dipendenti, **il caso ha avuto un impatto mediatico enorme**, spingendo Microsoft a rivedere parte delle proprie policy interne e ad avviare iniziative di culture reset.

- **Abolizione dello *stack ranking*** per ridurre la competitività tossica interna;
- **Implementazione di sistemi di *real-time sentiment analysis*** sulle comunicazioni aziendali, al fine di monitorare il clima interno;
- **Creazione di un *ombudsman* esterno** per la gestione indipendente di crisi reputazionali e segnalazioni sensibili;

Unilever - "Unstereotype alliance"
L'iniziativa di Unilever si è distinta per **l'approccio orientato alla supply chain**, estendendo gli standard di inclusione anche ai fornitori e partner:

- **Introduzione di clausole contrattuali *anti-harassment*** vincolanti per tutti i vendor;
- **Utilizzo di un sistema di blockchain-based reputation management**, volto ad assicurare trasparenza e responsabilità nella catena di fornitura;
- **Creazione di una piattaforma intersettoriale di *knowledge sharing***, per diffondere pratiche innovative e promuovere alleanze cross-industry.

Analisi comparativa delle strategie

Elementi comuni delle best practice

Le organizzazioni che si distinguono come più efficaci nel contrasto alla violenza di genere online presentano una serie di tratti condivisi. Si tratta di veri e propri **pilastri che consentono di trasformare le dichiarazioni di principio in pratiche concrete e misurabili**, grazie alla capacità di integrare leadership, tecnologia e collaborazione multi-attore in un unico modello organico.

Leadership commitment
L'impegno nasce dai vertici, con CEO e C-Suite che assumono la guida diretta delle iniziative. Questo si riflette sia nell'allocazione di budget consistenti - in media pari al 2,3% del fatturato nelle aziende leader - sia nell'integrazione di kpi specifici nei sistemi di valutazione e di compensazione dei manager, così da **legare la performance economica al raggiungimento degli obiettivi sociali.**

Technology integration
Le imprese più innovative fanno leva su strumenti avanzati come il ***Natural Language Processing*** per individuare l'uso di linguaggi inappropriati nelle comunicazioni digitali, il ***machine learning*** per riconoscere pattern sistemici di molestie e la ***blockchain*** per registrare in modo immutabile il completamento dei programmi formativi, al fine di **garantire tracciabilità e trasparenza.**

Multi-stakeholder approach
Valorizza la collaborazione con attori interni ed esterni. Le aziende più avanzate coinvolgono attivamente sindacati e rappresentanze dei lavoratori, stringono partnership con ONG e centri antiviolenza e instaurano un dialogo costante con le autorità regolatorie. Questo approccio consente di **rafforzare la legittimità delle politiche e di allinearle alle migliori pratiche internazionali.**

Framework di valutazione dell'efficacia

Un impegno strategico ha valore solo se è misurabile. Definire un framework di valutazione dell'efficacia consente infatti di capire cosa funziona e cosa è necessario migliorare, giustificando gli investimenti.

Kpi e metriche di misurazione
È necessario adottare **un cruscotto bilanciato di indicatori quantitativi** (per esempio percentuale di completamento dei programmi di formazione, tempi medi di risoluzione dei casi segnalati) e qualitativi (per esempio feedback raccolti tramite *focus group* o survey anonime).

Metodologie di impact assesment
Per una comprensione più profonda si possono utilizzare **studi longitudinali basati su sondaggi annuali**, analisi di business impact che correlano la percezione di sicurezza psicologica ai risultati aziendali, e raccolta di storie di impatto positivo per evidenziare benefici concreti.

Strumenti di reportistica e accountability
I dati raccolti devono confluire in **un report annuale** da presentare al senior management e al consiglio di amministrazione. Una versione aggregata e accessibile va condivisa con tutti i dipendenti, così da **rafforzare trasparenza e responsabilità diffusa.**

Parte VI
Raccomandazioni e prospettive future

Questa sezione finale distilla l'analisi in **una serie di raccomandazioni strategiche e operative per guidare le aziende** in un percorso di implementazione logico, realistico e sostenibile.

Raccomandazioni per le aziende

Checklist operativa per l'implementazione

Questa checklist riassume **i passaggi fondamentali della roadmap** per guidare il processo di implementazione.

Parte 1 **Fondamenta e impegno**

Ottenere sponsorship del CEO, costituire un gruppo di lavoro interfunzionale, condurre l'analisi dei rischi e l'audit delle policy.

Parte 2 **Sviluppo della governance e policy**

Sviluppare policy a tolleranza zero, definire procedure di segnalazione e investigazione, formalizzare un protocollo di supporto.

Parte 3 **Implementazione e formazione**

Lanciare una campagna di comunicazione, erogare la formazione a tutti i livelli (base, manager, bystander), implementare le soluzioni tecnologiche.

Parte 4 **Monitoraggio e miglioramento**

Definire e monitorare i KPI, condurre sondaggi periodici, produrre un report annuale e usare i dati per avviare un nuovo ciclo di miglioramento.

Timeline realistiche e resource allocation

Il cambiamento culturale richiede **tempo e un investimento adeguato di risorse.**

Timeline

Adottare un approccio a fasi **pluriennale.**

Breve Termine (primi sei mesi)

Gettare le fondamenta.

Medio Termine (12-18 mesi)

Costruire l'infrastruttura di policy e formazione.

Lungo Termine (dal secondo anno)

Radicare il cambiamento nella cultura.

Risorse

Allocare personale con tempo dedicato e **un budget specifico** per coprire i costi di tecnologia, formazione, supporto esterno alle vittime e comunicazione. Questo non è un costo, ma **un investimento strategico** in mitigazione del rischio, *talent retention* e *brand reputation*.

Integrazione con strategie di DE&I esistenti

La lotta alla violenza online non deve essere un'iniziativa isolata, ma va profondamente integrata nella **strategia di Diversità, Equità e Inclusione (DE&I).**

La sicurezza digitale è la nuova frontiera dell'inclusione: un ambiente di lavoro non è inclusivo se non è sicuro, anche digitalmente.

Collegamento con la parità di genere: il "soffitto di cristallo digitale" è un ostacolo concreto all'avanzamento delle donne, da affrontare all'interno delle strategie di gender equality.

Prospettiva intersezionale: riconoscere che le donne subiscono forme di violenza aggravate e specifiche a causa della molteplice appartenenza a diversi gruppi identitari discriminati (es. Donne di minoranze etniche; donne LGBTQIA+, ecc.), e per questo motivo necessitano di un supporto mirato.

Integrazione pratica: la governance, le metriche e la comunicazione sulla sicurezza digitale devono essere sinergiche e integrate con quelle della D&I.

Conclusioni e Bibliografia

In conclusione, la lotta alla violenza di genere online è una sfida complessa ma non eludibile, che interroga la responsabilità di ogni azienda. Affrontarla richiede **un impegno strategico, olistico e supportato dal vertice, che integri governance, policy, tecnologia e, soprattutto, una formazione continua.**

Non si tratta solo di mitigare un rischio, ma di **cogliere l'opportunità di costruire ambienti di lavoro digitali realmente sicuri, inclusivi e rispettosi**, dimostrando una leadership autentica e contribuendo a un cambiamento culturale di cui beneficiano tutti.

Bibliografia e Risorse

- **Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali** (Digital Services Act - DSA), *Gazzetta ufficiale dell'Unione europea*
- **Parlamento Europeo** (2021). *Combating gender-based cyber-violence*. European Parliamentary Research Service, EPRS_ATA(2021)698830_EN
- **Commissione Europea** (2024). *Digital Services Act: Questions and Answers*. Shaping Europe's digital future. Disponibile su: https://digital-strategy.ec.europa.eu
- **Center for Democracy and Technology Europe** (2025). *Online Gender-Based Violence in the EU: What Now?*. CDT Europe Policy Brief

Normativa e Fonti Istituzionali Italiane

- **Decreto-legge 23 luglio 2019, n. 69** (*Codice Rosso*), convertito con modificazioni dalla legge 19 luglio 2019, n. 69
- **Decreto Legislativo 8 giugno 2001, n. 231** - Disciplina della responsabilità amministrativa delle persone giuridiche
- **Codice Penale**, Art. 612-ter (Diffusione illecita di immagini o video sessualmente espliciti)

Fonti Istituzionali Internazionali

- **U.S. Equal Employment Opportunity Commission** (2016). *Select Task Force on the Study of Harassment in the Workplace: Report of Co-Chairs*. EEOC
- **International Labour Organization** (2019). *Convention C190 - Violence and Harassment Convention*
- **UN Global Compact** (2020). *Women's Empowerment Principles - Equality Means Business*

Ricerca Accademica e Studi Peer-Reviewed

- **Chirico, F., et al.** (2024). "Gender-based violence and harassment at work and health and occupational outcomes: A systematic review of prospective studies". *BMC Public Health*, 24, 1904. https://doi.org/10.1186/s12889-024-19304-0
- **Raj, A., Johns, N.E., Jose, R.** (2020). "Gender Parity at Work and Its Association With Workplace Sexual Harassment". *American Journal of Preventive Medicine*, 58(4), 725-730
- **Thompson, L.F., Romo, L.F.** (2024). "Sexual Harassment at Work: Scoping Review of Reviews". *International Journal of Environmental Research and Public Health*, 21(4), 498
- **Kumar, P., et al.** (2024). "A gender-based review of workplace violence amongst the global health workforce—A scoping review of the literature". *PLOS Global Public Health*, 4(7), e0003336
- **Bondestam, F., Lundqvist, M.** (2020). "Sexual harassment in higher education – a systematic review". *European Journal of Higher Education*, 10(4), 397-419

Report e Studi Settoriali

- **New America Foundation** (2019). *Sexual Harassment: A Severe and Pervasive Problem*. Better Life Lab Report
- **Gallup Inc.** (2025). *Global Study: 23% of Workers Experience Violence, Harassment*. World Poll Survey
- **National Sexual Violence Resource Center** (2020). *Ending Sexual Assault and Harassment in the Workplace*. NSVRC Policy Brief

Analisi Giuridico-Accademiche Specializzate

- **Mihr, A.** (2022). "An Intersectional Lens on Online Gender Based Violence and the Digital Services Act". *Verfassungsblog on Constitutional Matters*. https://verfassungsblog.de/dsa-intersectional/
- **University of Chicago Law School** (2024). "The Digital Services Act and the EU as the Global Regulator of the Internet". *Chicago Journal of International Law*, 25(1)
- **Algorithm Watch** (2024). *A guide to the Digital Services Act, the EU's new law to rein in Big Tech*. Policy Analysis Report

Risorse per Supporto e Implementazione Aziendale

- **Telefono Rosa** - Numero nazionale anti-violenza e stalking: 1522
- **D.i.Re - Donne in Rete contro la violenza** - Rete nazionale centri antiviolenza
- **PermessoNegato** - Associazione per i diritti e le libertà digitali: https://www.permessonegato.it
- **Salesforce Equality Hub** - Best practice e toolkit per aziende
- **Microsoft Digital Safety Content Hub** - Risorse per workplace digital safety

Novembre 2025

www.valored.it