"Annali online della Didattica e della Formazione Docente"
Vol. 16, n. 27/2024, pp. 26-64 – ISSN 2038-1034

Stupri digitali: una questione di governance del cyberspazio

Enrico Maestri

Abstract – *In this essay, I argue that online gender violence is not primarily due to cultural or linguistic causes. Both gender and cultural studies fail to locate the real causes of digital gender violence in cultural patterns and linguistic performances. Contrary to the prevailing theoretical positions in the literature on online gender violence, I argue that the deep roots of this violence on the web are a direct consequence of the kind of governance that regulators allow Internet Service Providers, the real controllers of cyberspace, to engage in. The central thesis of this article is that effective regulation of digital gender-based violence requires a structural approach based on digital communities, abandoning the idea of adapting real-world laws to cyberspace. In short, this essay focuses on the structure of digital architecture rather than cultural forms of gender in order to better understand the workings of power and the production of collective subjectivities in relation to gender, sexuality, and other types of social relations.*

Riassunto – *In questo saggio sostengo che la violenza online di genere non sia principalmente attribuibile a cause culturali o linguistiche. Tanto i gender studies quanto i cultural studies non riescono a individuare le vere cause della violenza digitale di genere nei pattern culturali e negli atti performativi linguistici. Diversamente dalle posizioni teoriche prevalenti nella letteratura sulla violenza di genere online, sostengo che le radici profonde di questa violenza nel web siano direttamente conseguenza del tipo di governance permessa dai regolatori agli Internet Service Providers (ISP), i veri controllori del cyberspazio. La tesi centrale di questo articolo sostiene che, per rendere efficace la regolamentazione della violenza digitale di genere, è necessario adottare un approccio strutturale basato sulle comunità digitali, abbandonando l'idea di adattare le leggi del mondo reale al cyberspazio. In sintesi, questo saggio, invece di concentrarsi sulle forme culturali di genere, pone l'accento sulla struttura dell'architettura digitale per una migliore comprensione del funzionamento del potere e della produzione di soggettività collettive in relazione al genere, alla sessualità e ad altri tipi di relazioni sociali.*

Keywords – gender-based violence, digital violence, cybercrime, lex algorithmica, cyberstalking, digital communities

Parole chiave – violenza di genere, violenza digitale, crimine informatico, lex algoritmica, cyberstalking, comunità digitali

Enrico Maestri (PhD) è Professore associato di Filosofia del diritto presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Ferrara. Attualmente, ricopre diversi insegnamenti, tra cui *Diritto dell'ambiente informatico, Teoria generale del diritto, Conoscenza e didattica del diritto, Metodologia e logica giuridica*. Inoltre, è anche titolare della cattedra di Etica e diritto dell'intelligenza artificiale nel corso di laurea magistrale in Intelligenza Artificiale, Data Science e Big Data presso il Dipartimento di Informatica. Tra le sue recenti pubblicazioni: *FEMtech e l'avvento della medicina pervasiva: incubo o nobile sogno?* (in "BioLaw Journal-Rivista di BioDiritto", 2023); *Legal surrogacy in question. Discussing with ChatGPT* (in "Medicina Historica", 2023); *Broken Justice: Justice and Relativism in the Work of Friedrich Dürrenmatt* (in "Pólemos", 2022); *Surveillance and Profiling. Online Person's Privacy Between Criminogenic Structures and Legal Paternalism* (in "Journal of Ethics and Legal Technologies", 2021).

L'articolo è riconducibile alle tematiche del Progetto di Ricerca di Interesse Nazionale (PRIN 2022) *New Frontiers for a Participatory Criminal Justice Towards the Thresholds of Metaverse*, finanziato dal MUR e coordinato dalla Prof.ssa Benedetta Galgani dell'Università di Pisa e del Fondo di Incentivazione alla Ricerca Dipartimentale (FIRD 2023) *Educare alla dignità nell'era digitale*, finanziato dall'Università degli Studi di Ferrara.

1. Introduzione

Con il progressivo sviluppo della società umana, anche la sua struttura sociale ha subito un'evoluzione nel corso del tempo. Dall'Illuminismo, che valorizzava la ragione, si è transitati all'età industriale moderna, contraddistinta dalla tecnologia e orientata all'efficienza utilitaristica[1]. Attualmente ci troviamo immersi nell'era della società dell'informazione[2], in cui le informazioni vengono elaborate e diffuse tramite reti elettroniche.

L'avvento dell'era dell'informazione ha portato a un notevole sviluppo della comunicazione, dando origine a relazioni interpersonali sempre più virtuali, spesso mediate dai social network. Questo cambiamento ha determinato una trasformazione delle relazioni tradizionali, con un aumento dell'anonimato e una riduzione delle interazioni fisiche[3].

L'introduzione di Internet e dei dispositivi digitali ha altresì favorito l'emergere di nuove forme di criminalità online, come lo stalking informatico, la diffamazione online, il morphing, lo spoofing di e-mail, la pornografia virtuale, la diffamazione sessuale online, il bullismo online, il cyber hacking, il cyber bullismo e altre forme ancora.

I gruppi vulnerabili, in particolare le donne e gli adolescenti, sono particolarmente esposti a queste forme di criminalità. La violenza digitale comprende tutti gli atti di violenza di genere perpetrati attraverso l'utilizzo delle tecnologie digitali dell'informazione e della comunicazione. Questo fenomeno complesso e in crescita sta emergendo sui social network, sfidando i governi a intervenire con determinazione. Di conseguenza, la criminalizzazione della violenza digitale sta diventando una tendenza normativa diffusa a livello globale[4]. La regolamentazione di tale violenza si trova ad affrontare numerose sfide a causa degli attori coinvolti, dei conflitti normativi e delle questioni di giurisdizione nazionale su Internet[5].

Numerose donne sono vittime di varie forme di violenza digitale che si trasformano in autentici stupri digitali: le loro immagini intime vengono diffuse senza consenso dagli ex partner come

[1] D. Schiller, *Digital Capitalism. Networking the Global Market System*, Cambridge (MA), The Mit Press, 2000.

[2] M. Castells, *The power of identity*, London, John Wiley & Sons, 2011; trad. it. *Il potere delle identità*, Milano, EGEA, 2014.

[3] V. Miller, *Understanding Digital Culture*, London, SAGE Publications, 2011.

[4] N. Henry, A. Powell, *Sexual violence in the digital age: The scope and limits of criminal law*, in "Social & Legal Studies", 25(4), 2016, pp. 397-418.

[5] M. Weber *et al.*, *Online hate does not stay online–how implicit and explicit attitudes mediate the effect of civil negativity and hate in user comments on prosocial behaviour*, in "Computers in human behaviour*",* 104, 2020, pp. 106-192.

strumento per controllare il loro corpo. Al contempo, le donne che denunciano l'impunità per chi commette violenza di genere rischiano di subire migliaia di minacce di violenza sessuale online per intimidirle. Questi casi possono essere collegati a due tesi presenti nella letteratura sulla violenza di genere: primo, la violenza contro le donne mira a erodere la coesione sociale e a rafforzare la loro subordinazione[6]; secondo, la violenza è spesso perpetrata contro le donne attive nella sfera politica per escluderle dalla partecipazione pubblica[7]. L'uso sempre più diffuso di Internet ha amplificato questa forma di violenza contro le donne, rendendola più evidente e ponendo nuove sfide alla sua regolamentazione.

Le peculiarità uniche del cyberspazio, come la globalizzazione, l'assenza di confini territoriali, l'anonimato degli utenti e la facilità di impersonificazione, hanno creato le condizioni affinché i criminali possano minacciare gli individui online allo stesso modo che nel mondo reale. In un'era dominata dalle tecnologie digitali, l'interazione tra hardware e software dà vita a un mondo quasi fantascientifico, senza confini geografici definiti. Le società contemporanee sono fortemente influenzate dalla tecnologia digitale, che genera uno spazio virtuale dinamico attraverso le reti informatiche. Questo spazio virtuale è conosciuto come cyberspazio. Pur essendo una costruzione immateriale, il cyberspazio può essere percepito, udito e interagito. È caratterizzato da dinamicità, indefinito e in costante espansione; non esiste in isolamento ma è strettamente interconnesso con il mondo fisico.

Le attività precedentemente svolte nello spazio fisico sono state trasferite nel cyberspazio, portando alla scoperta di nuove forme di criminalità che mirano alle fasce vulnerabili della società[8].

Le azioni illecite che prendono di mira le donne e le adolescenti nell'ambiente online rappresentano una delle minacce principali e più pericolose in questo spazio. La violenza esercitata contro le donne online ha gravi conseguenze sulla loro salute fisica e mentale, rafforzando la discriminazione di genere e violando i loro diritti fondamentali. Le donne che subiscono molestie e abusi nel cyberspazio spesso esitano a cercare assistenza legale, talvolta rinunciando e concedendo agli autori un'altra opportunità di danneggiare le loro vite. Le motivazioni dietro questa riluttanza possono variare, da inibizioni sociali o personali alla perdita di fiducia nei rimedi giuridici disponibili.

[6] G. Bardall, E. Bjarnegård, J.M. Piscopo, *How is political violence gendered? Disentangling motives, forms, and impacts*, in "Political Studies", 68(4), 2020, pp. 916 ss.

[7] J.R. Sanín, *Violence against women in politics: Latin America in an era of Backlash*, in "Signs", 45(2), 2020, pp. 302 ss.

[8] Ad avviso di Deborah Lupton, ha poco senso continuare a parlare di cyberspazio: la computazione ubiqua ha reso virtuale quasi tutta la realtà. Non ci muoviamo più tra online e offline: le nuove tecnologie locative anziché condurci nello cyberspazio ci identificano con il luogo e con lo spazio in cui viviamo. Cfr. D. Lupton, *Sociologia digitale*, Milano-Torino, Pearson, 2018, p. 139. Contrariamente a questa tesi, ritengo che il concetto di cyberspazio mantenga la sua utilità euristica. Il cyberspazio è un sistema cibernetico comunicativo e trasformativo: è uno spazio senza luoghi e senza corpi. All'interno di questo sistema non esistono agenti morali o persone che agiscono con più o meno ampi margini di libertà: le persone sono solo mere unità funzionali del sistema cibernetico. Le persone non sono solamente e sempre 'offlife' e ugualmente non sono solo soggetti che vivono e agiscono 'onlife'; questo approccio finisce per ripetere l'errore di Cartesio, per il quale il lato informazionale guida la carcassa biologica dell'essere umano.

Attualmente, sia a livello nazionale che internazionale, manca una legislazione adeguata che specifichi la protezione delle donne online. Oltre alle leggi e alle istituzioni giuridiche, la risoluzione degli abusi e delle molestie nel cyberspazio deve essere ricercata nei valori sociali, nelle norme e nella determinazione dei professionisti e degli attivisti nel contrastare questa minaccia. Il diffuso stigma sociale derivante dalla diffusione di contenuti osceni o pornografici, inclusi video o immagini manipolate, costringe talvolta le donne a compiere atti sessuali sotto minaccia di divulgazione.

La criminalità informatica contro le donne costituisce una seria minaccia per la sicurezza individuale nel suo complesso. La questione della validità delle leggi online e della regolamentazione delle attività su internet è ancora oggetto di dibattito e sarà il fulcro di questo articolo. Seguiranno alcuni paragrafi che esplorano l'architettura normativa del cyberspazio, evidenziandone la natura discriminatoria e criminogena.

Testerò questa tesi esaminando una delle forme più insidiose e invasive di violenza digitale, il cyberstalking, mettendo in luce le differenze tra lo stalking fisico e il cyberstalking e come queste differenze influenzino la loro regolamentazione. Il mio interesse non è tanto nella progettazione di riforme giuridiche formali, ma piuttosto in un approccio più strutturale alla regolamentazione del cyberstalking. È fondamentale adottare una regolamentazione basata su una comprensione approfondita dell'architettura del mondo digitale e, di conseguenza, su una maggiore consapevolezza della natura e delle manifestazioni del comportamento violento.

Non intendo suggerire che la revisione delle leggi esistenti non sia importante. Ma, nel contesto del crimine informatico, il potenziale di miglioramento del diritto internazionale e nazionale si è rivelato deludente[9]. I critici argomentano che attualmente il cyberspazio è sovraccarico di leggi che spesso mancano di prove concrete della loro efficacia nel garantire un comportamento legale da parte degli utenti[10]. Le riforme legislative sono state ostacolate e limitate dalla capacità del codice informatico di influenzare la legislazione tradizionale.

In generale, le attività criminali online non solo replicano quelle del mondo fisico, ma sviluppano anche caratteristiche uniche, alimentate dall'anonimato che caratterizza questo ambiente[11]. Inoltre, le nuove tecnologie sociali hanno modificato profondamente l'architettura sottostante le interazioni sociali e la diffusione delle informazioni.

L'analisi proposta in questo articolo illustrerà le inadeguatezze dei tradizionali approcci giuridici (*ex post facto*) alla regolamentazione e alla prevenzione della violenza digitale[12]. E offrirà una soluzione strutturale al problema, basandosi sulla concezione di comunità virtuali elaborata da Howard Rheingold nel suo libro, *The Virtual Community*, pubblicato nel 1993.

[9] L. Lessig, *The law of the horse: what cyberlaw might teach*, in "Harvard Law Review", 113, 1999, p. 501 ss.

[10] Id., *Code: And Other Laws of Cyberspace*, New York, ReadHowYouWant, 2009.

[11] R. Botsman, *Who Can You Trust? How Technology Brought Us Together and Why It Might Drive Us Apart*, New York, PublicAffairs, 2017.

[12] R.S. McNeal *et al.*, *Cyber Harassment and Policy Reform in the Digital Age: Emerging Research and Opportunities*, New York, IGI Global, 2018.

2. Le architetture criminogene della Rete

In Internet operano due livelli normativi complementari. Un livello più profondo ed efficace, sovrainclusivo dei casi regolati, che definisco come diritto a matrice tecnologica: il diritto di Internet, noto come "Code is law". A questo livello normativo, composto da regole tecniche, i fornitori di servizi guidano i comportamenti degli utenti. Il sistema informatico agisce come un filtro delle aspettative, con un effetto di feedback che genera conseguenze digitali amplificate e disciplinate tecnologicamente in modo diverso rispetto all'ambiente offline.

Il secondo livello normativo è più superficiale ed esornativo, sottoinclusivo dei casi regolati, chiamato diritto a matrice deontica: il diritto per Internet, noto come "Law is code". A questo livello normativo, composto da regole giuridiche deontiche, gli Stati esonerano i fornitori da una responsabilità generale sui contenuti caricati e gestiscono i dati degli utenti attraverso azioni come raccolta, trattamento, deframmentazione, filtrazione e profilazione. Queste attività si basano sul consenso degli interessati e su una forma di responsabilizzazione preventiva che coinvolge sia i titolari dei dati sia gli utenti.

È importante sottolineare che la regolamentazione tecnica è definita dai proprietari e dai fornitori di servizi online. Questa regolamentazione definisce l'architettura di Internet e stabilisce le modalità di accesso ai servizi offerti dagli ISP, influenzando significativamente la libertà di espressione e la privacy degli utenti. Ad esempio, molti social network impongono agli utenti di rinunciare al diritto di utilizzare le proprie immagini e contenuti a fini commerciali. Inoltre, molti ISP raccolgono dati per scopi pubblicitari o di profilazione senza offrire agli utenti un adeguato controllo sui propri dati personali[13].

La complessità della tecnologia rende difficile per la legislazione tradizionale tenere il passo con l'evoluzione di Internet. Questo fenomeno implica un avvolgimento del mondo attorno alle tecnologie digitali che possono essere considerate come di terzo ordine, capaci di operare sulla base della rappresentazione della realtà determinata dai dati online elaborati in modo specifico. Le tecnologie digitali contribuiscono in modo sempre più pervasivo a definire l'ambiente in cui gli esseri umani vivono e interagiscono.

Il passaggio da strumento a ambiente dovrebbe farci comprendere che le tecnologie digitali, attraverso il loro potere computazionale, contribuiscono a plasmare l'ambiente in cui viviamo garantendo le condizioni della loro stessa esistenza indipendentemente[14] dagli esseri umani. La codifica computazionale del diritto segna in modo irreversibile la crisi della sovranità statale: la rigidità del diritto tradizionale si rivela incapace di regolare le nuove modalità delle azioni umane; la destatualizzazione e la deterritorializzazione producono un diritto flessibile adattabile al modello reticolare del mondo digitale.

[13] A. Monti, R. Wacks, *Protecting Personal Information: The Right to Privacy Reconsidered*, London, Bloomsbury Publishing, 2019.

[14] M. Durante, *Potere computazionale: L'impatto delle ICT su diritto, società, sapere*, Milano, Mimesis, 2019.

Aderendo ad un approccio che gli anglosassoni designano con l'espressione *code-based approach*[15], elaborato da Lawrence Lessig[16] e da Joel Reidenberg[17], io ritengo che l'architettura del cyberspazio non sia fissata *by default*, bensì in funzione del suo *code*[18]. Il *code* è mutevole: potrebbe essere il governo o il mondo delle multinazionali a determinarne una sua particolare evoluzione. L'architettura del cyberspazio non è neutrale. Laddove le architetture del *code* incidono sui vincoli giuridici, esse finiscono per soppiantare anche i valori e i principi fondamentali del diritto. Nel caso della proprietà intellettuale, ad esempio, il *code* appare *sovrainclusivo* rispetto alla legge: quest'ultima favorisce un'implementazione architettonica del *code* tale da favorire i detentori di cospicue percentuali di proprietà intellettuale, così esentando le multinazionali delle telecomunicazioni dalle responsabilità di servizio universale e di condivisione delle reti. Nel campo del *copyright* l'architettura digitale, cioè il modo con cui le tecnologie disegnano *ex ante* lo spazio di comportamento degli utenti, ha progressivamente ristretto i margini di libertà (*fair use*) delle scelte individuali. L'architettura, rappresentata dal sistema numerico binario[19], è diventata un vincolo fortissimo per l'individuo, massimamente invasiva delle sue capacità di azione: la proprietà digitale, ad esempio, è una forma di comunicazione che diviene proprietà mimetica dell'architettura (ogni utilizzo di un'opera creativa si trasforma automaticamente in una copia) e pone ora controlli e regole, influendo su legge e mercato. Diversamente dai controlli introdotti per legge, quelli inseriti dalla tecnologia non formano oggetto di verifica giudiziale[20]. D'altronde, mentre la regola legislativa (aspettativa d'azione) risulta verificabile e contestabile, altrettanto non può dirsi per la regola tecnologica che si presenta all'utente come una aspettativa di comunicazione[21].

Più semplicemente, Internet è governato da regole tecniche del tipo "se vuoi R, allora devi necessariamente fare S"[22]. Se un atto non adempie ad un dovere tecnico non ottiene il fine che

[15] R.H. Weber, *Realizing a New Global Cyberspace Framework. Normative Foundations and Guiding Principles*, Berlin, Springer, 2015, pp. 53 ss.

[16] L. Lessig, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999.

[17] J.R. Reidenberg, *Technology and Internet Jurisdiction*, in "University of Pennsylvania Law Review", 153, 2005, pp. 1951 ss.

[18] E. Maestri, *Lex informatica: diritto, persona e potere nell'età del cyberspazio*, Napoli, Edizioni scientifiche italiane, 2015.

[19] Ad avviso di Luhmann, i codici binari sono regole di duplicazione in modo tale che l'informazione, nel processo di comunicazione, viene valutata e confrontata con un controvalore precisamente corrispondente con esclusione di terze possibilità; cfr. N. Luhmann, *Comunicazione ecologica*, Milano, FrancoAngeli, 1989, p. 107. Ed ancora, la selettività di una comunicazione viene attribuita a se stessa: è essa che costituisce il proprio senso, e gli interessati reagiscono con scelte comportamentali proprie non in base a soluzioni prefissate, bensì in base a informazioni su prestazioni selettive altrui; cfr. Id., *Procedimenti giuridici e legittimazione sociale*, Milano, Giuffrè, 1995, p. 33.

[20] L. Lessig, *Cultura libera: un equilibrio fra anarchia e controllo, contro l'estremismo della proprietà intellettuale*, Milano, Apogeo, 2007, pp. 124 ss.

[21] R. Caso, *L'«immoralità» delle regole tecnologiche: un commento alle teorie degli studiosi Burk e Gillespie*, in G. Ziccardi (a cura di), *Nuove tecnologie e diritti di libertà nelle teorie nordamericane*, Modena, Mucchi, 2008, p. 38 ss.

[22] G. Gometz, *Le regole tecniche. Una guida refutabile*, Pisa, ETS, 2008.

si propone. In Internet le proposizioni normative sono regole tecniche di modo che il nesso di consequenzialità non preveda la disobbedienza: sono atti comunicativi produttivi di effetti nel momento in cui e per il fatto che vengono enunciati. La norma tecnica non prescrive l'adattamento ma lo attua.

La società è invece generalmente governata da regole condizionali prescrittive del tipo "se è X, allora deve essere Y". Si tratta di comportamenti da tenere ma declinati in termini condizionali deontici sicché non sono stati messi in atto al momento della prescrizione (che può ben essere disattesa). La norma deontica prescrive l'adattamento, non lo attua né le interessa che sia attuato.

In questo senso, ad avviso di Luhmann, le norme deontiche o prescrittive a differenza di quelle tecniche non costringono (non pongono, non presuppongono, non costituiscono) alle condotte conformi, bensì proteggono contro chi non vi si adatta. Laddove questa protezione sia difficoltosa, il diritto tende a deflazionarsi socialmente[23]. È questo esattamente il caso dell'ambiente digitale.

La "non regolabilità" della Rete è un'arma a doppio taglio. Da un lato, rappresenta una virtù, in quanto tutela la libertà di parola e facilita la libera circolazione di informazioni e idee. Essa rappresenta una sorta di Primo Emendamento digitale, che rende difficoltoso per i governi controllare il flusso di informazioni. Questo è evidente in contesti come l'Ucraina o Gaza, dove la Rete permette la libera diffusione di notizie e immagini, anche in presenza di regimi repressivi.

Dall'altro lato, la "non regolabilità" può essere un vizio, in quanto rende difficoltoso contrastare la diffusione di contenuti illegali e dannosi, come la pornografia infantile o l'incitamento all'odio. La Rete rende difficoltoso per i governi europei applicare le leggi contro il linguaggio nazista online, permettendo la diffusione di ideologie discriminatorie e xenofobe. La "non regolabilità" facilita la diffusione di materiale pedopornografico online, ostacolando l'identificazione e la punizione dei responsabili.

In questi casi, l'architettura della Rete disabilita la regolamentazione, ostacolando l'azione delle autorità e creando un terreno fertile per la proliferazione di materiale illegale e pericoloso.

Tra il provider della struttura informatica e gli utenti si realizza un implicito baratto: l'utente che vuole utilizzare la piattaforma del provider e creare il suo spazio virtuale deve "consensualmente" cedere i propri dati al provider proprietario della piattaforma.

Ciò comporta una vera e propria mutazione genetica del trattamento dei dati e della loro concezione, poiché essi entrano a fare parte di quella immensa rete di calcolo che è Internet, passando da componente fondamentale per la costruzione della *personalità digitale* dell'individuo a valore immateriale di scambio.

Paradossalmente, i codici tradizionali di condotta giuridica ("Law is code") hanno favorito la costruzione di Internet come ambiente criminogeno perché hanno sottovalutato la forza normativa incorporata nelle tecnologie digitali ("Code is law"): quest'ultime consentono alle persone di esprimere e di mostrare "il lato oscuro delle persone" senza alcun scrupolo. In una reale società civile, operano varie norme giuridiche e norme sociali, scritte o non scritte, che limitano la parola

[23] N. Luhmann, *Esistono ancora norme fondamentali?*, Roma, Armando, 2011.

e il comportamento delle persone, ma la popolarità di Internet, cioè la sua forza normativa tecnica basata sullo slogan "prendere o lasciare" ha totalmente rivoluzionato il modo in cui le persone comunicano e si trasformano[24].

Le conseguenze etico-giuridiche di questa pluralità dei livelli normativi operanti nell'ambiente digitale sono una doppia colpevolizzazione della vittima: vittima dei providers da cui dipende (Facebook, Instagram e Tik Tok sono generatori di dipendenza) e vittima dei regolatori da cui è criminalizzata.

Con lo sviluppo graduale della comprensione di Internet, sono così emerse diverse fonti di vulnerabilità, note in letteratura come i "tre punti di vulnerabilità di Internet"[25]: anonimato, convenienza e accessibilità. Più recentemente, sono state suggerite altre vulnerabilità, come l'approssimazione al mondo reale[26], una maggiore accettabilità online di attività inaccettabili nel mondo reale[27], l'ambiguità tra morale e crimine[28] e una distanziazione tra il sé reale e il sé online.

Una caratteristica strutturale di Internet che interagisce con queste vulnerabilità è la sua natura essenzialmente non gerarchica. Sebbene l'accesso, l'hosting e la ricerca di servizi siano mediati da agenzie di servizi Internet commerciali e governative, il contenuto di Internet dipende principalmente dall'attività degli utenti poiché è la struttura che la favorisce.

Il social networking, ad esempio, è diventato una forma di comunicazione onnipresente tra i giovani. Permette contatti rapidi e multipli tra le persone, senza limitazioni geografiche o costi, con risultati benefici, ma può anche contribuire a un maggiore rischio di danni.

Le caratteristiche delle piattaforme di social networking modellano o consentono pratiche e usi specifici, che l'utente può modificare anche attraverso le impostazioni e l'uso, come l'utilizzo di più account[29].

Ciò crea un ambiente dinamicamente complesso in cui sia il destinatario che il mittente della comunicazione partecipano reciprocamente. Il modo in cui queste piattaforme vengono utilizzate è correlato al rischio di danni[30]. Alcune attività, come avere un profilo pubblico prominente, un numero elevato di contatti o visualizzare informazioni identificative, aumentano particolarmente il rischio di danni ai bambini, incluso il contatto da parte di terzi.

[24] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, New Jersey, Princeton University Press, 2011.

[25] A.I. Cooper (Ed.), *Sex and the Internet: A guidebook for clinicians*, London, Brunner-Routledge, 2020.

[26] M.W. Ross, *Men who have sex with men, and the Internet: Emerging clinical issues and their management*, in A.I. Cooper (ed.), *Sex and the Internet: A guidebook for clinicians*, cit.

[27] S.A. King, *Internet gambling and pornography: Illustrative examples of psychological consequences of communication anarchy*, in "Cyberpsychology & Behavior*", 2*, 1999, pp. 175-193.

[28] K.M. Hertlein, A. Stevenson, *The Seven "As" Contributing to Internet-Related Intimacy Problems: A Literature Review. Cyberpsychology, in* "Journal of Psychosocial Research on Cyberspace", *4*, 2010, article 3.

[29] S. Livingstone *et al.*, *Risks and safety on the internet. The perspective of European children: Full findings*, http://eprints.lse.ac.uk/33731/, 2011; consultato in data 6 febbraio 2024.

[30] E. Quayle, M. Taylor, *Social networking as a nexus for engagement and exploitation of young people*, in "Information Security Technical Report", 16, 2011, pp. 44 ss.

In effetti, il modo in cui i siti di social networking vengono utilizzati è probabilmente più importante in termini di esperienza di rischio di danni rispetto all'uso stesso dei siti di social networking[31]. Ad esempio, in un contesto più specifico, comportamenti sessuali a rischio elevato tra i giovani possono essere associati a una maggiore attività online.

Il modo in cui i siti di social networking influenzano il comportamento può essere utilmente concettualizzato in termini di *affordances* e apprendimento collaborativo offerti da tali siti[32].

Gli "amici" su Facebook, ad esempio, sono vettori, il cui accumulo è segno di socialità; analogamente, sui social media un tweet è un vettore, e l'accumulo di "follower" è un obiettivo di molti utenti dei social media.

Internet è stato utilizzato per creare uno spazio privato in cui coinvolgersi in comportamenti sessuali intenzionali con i giovani. Questo coinvolgimento è stato per alcuni solo un sostegno alla fantasia, ma per altri è stato un precursore di un'aggressione sessuale offline e della predazione sessuale online tramite Internet. Le opportunità offerte dalle piattaforme Internet non solo hanno consentito l'accesso ai giovani, ma hanno anche facilitato l'acquisizione rapida di competenze[33].

I devices digitali sono stati trasformati in psico-dispositivi di iper-captazione dell'attenzione[34], o meglio, della produzione industriale della disattenzione.

Se vi è sempre stata captazione dell'attenzione, ed essa è essenziale alla formazione dell'intelligenza, oggi il rischio è una sua deformazione radicale, per cui l'attenzione profonda, caratteristica dell'apprendimento riflessivo, letterario, scientifico e, in generale, critico, sembra essere man mano sostituita dalla *hyper-attention*, un'attenzione sempre più diffusa tra i cosiddetti "nativi digitali", direttamente connessa al multitasking e che, è caratterizzata da rapide oscillazioni tra differenti compiti e molteplici flussi di informazione, alla ricerca di un sempre più elevato livello di stimolazione e dalla conseguente debole tolleranza per la noia. Bernard Stiegler mette in luce come l'iper-attenzione nasconda, nel superlativo, una iper-sollecitazione e una iper-captazione della stessa attenzione che, a forza di essere stimolata, giungerebbe paradossalmente a dissiparsi e a perdere il carattere di profondità, guadagnato con le pratiche riflessive e contemplative connesse alla psicotecnica letteraria[35]. In tal senso, l'iper-attenzione è una forma di attenzione non solo necessaria a un utilizzo multitasking delle nuove tecnologie mediatiche, ma è anche plasmata da queste ultime. Per usare il vocabolario degli esperti di telemarketing, in quanto oggetto di compravendita, l'iper-attenzione rappresenta il nutrimento privilegiato delle industrie di servizi e del marketing, che ha di mira principalmente la gioventù e che capta in modo massivo l'attenzione dei bambini fin dalla loro più giovane età, fino al punto di dissiparsi e regredire all'inumanità, ossia ad un livello di semplice soddisfacimento dell'indole pulsionale dei soggetti.

[31] E. Staksrud *et al.*, *Does the use of social networking sites increase children's risk of harm?*, in "Computers in human behaviour", 29, 2013, pp. 40 ss.

[32] R. Thomas, E. Christiansen, *Community and social network sites as Technology Enhanced Learning Environments*, in "Technology, Pedagogy and Education", 17, 2008, pp. 207 ss.

[33] E. Quayle *et al.*, *Rapid skill acquisition and online sexual grooming of children*, in "Computers in Human Behavior", 39, 2014, pp. 368 ss.

[34] B.J. Fogg, *Tecnologia della persuasione*, Milano, Apogeo, 2005.

[35] B. Stiegler, *Prendersi cura. Della gioventù e delle generazioni*, Napoli, Ortothes, 2014.

L'essenza dell'argomento presentato qui è che il comportamento problematico su Internet, in qualsiasi forma, è almeno sostenuto, se non addirittura creato, dal modo in cui interagiamo con la rete. Un aspetto critico di questo fenomeno potrebbe essere rappresentato da ciò che è stato definito come "disinibizione online" e dal modo in cui può influenzare stati emotivi intensificati.

La disinibizione online si riferisce al modo in cui alcune persone tendono a rivelarsi o ad agire più frequentemente o intensamente rispetto a quanto farebbero di persona[36].

Ad avviso di Suler, ci sono sei fattori che interagiscono tra loro per creare questo effetto: anonimato dissociativo, invisibilità, asincronicità, introiezione solipsistica, immaginazione dissociativa e minimizzazione dell'autorità. Inoltre, sappiamo che la divulgazione di informazioni personali avviene più rapidamente nella comunicazione mediata da Internet rispetto a quella offline e che il potenziale di vulnerabilità psicologica che ne deriva offre un mezzo per comprendere come l'interazione su Internet possa portare a comportamenti che sarebbero improbabili o meno frequenti offline[37]. La nostra esperienza di Internet è essenzialmente quella di un mezzo performativo dinamico, e potrebbe essere necessario rivalutare il nostro concetto di rischio in relazione a ciò[38].

La mia analisi dunque giustifica l'ipotesi che Internet abbia qualità criminogene. Questa potrebbe essere una conclusione plausibile per due ragioni. In primo luogo, la natura distribuita di Internet e la mancanza di controllo *ex ante facto* sui contenuti contribuiscono a una maggiore disponibilità di materiale illegale o indesiderabile. In secondo luogo, lo sviluppo di complessi microsistemi globali distribuiti aumenta effettivamente le opportunità di accesso a tali contenuti, molti dei quali possono essere illegali.

3. Vigilanza algoritmica

La vigilanza algoritmica consiste in una sorveglianza diffusa, che fa parte di un sistema più ampio rispetto ai classici sistemi panottici di sorveglianza[39]. Questo concetto non è nuovo per la maggior parte delle piattaforme social, su cui si è scritto molto riguardo ai loro modelli di business della sorveglianza[40], anche se alcune aree della sorveglianza delle piattaforme sono state meno esplorate, come il controllo in coerenza con i termini di servizio, gli standard della comunità e altre politiche delle piattaforme. Il controllo algoritmico basata sulla sorveglianza coinvolge il tracciamento pervasivo e l'analisi dei metadati che descrivono il comportamento

[36] J. Suler, *The online disinhibition effect*, in "Cyberpsychology & Behavior", 2004, pp. 321 ss.

[37] S. Turkle, *Il disagio della simulazione*, Milano, Ledizioni, 2011.

[38] E. Montelius, K. Nygren, *Doing' risk, 'doing' difference: towards an understanding of the intersections of risk, morality and taste*, in "Health, Risk & Society", 16, 2014, pp. 431 ss.

[39] D. Lyon, *Surveillance studies: An overview*, London, Polity Press, 2007.

[40] S.C. Koch *et al.*, *Body Memory, Metaphor and Movement*, Amsterdam, John Benjamins Publishing Company, 2012.

degli utenti in relazione al contenuto, ad altri utenti e alla piattaforma stessa, al fine di utilizzare queste informazioni per tentare di modificarne il comportamento desiderato[41].

Foucault sosteneva che le *governamentalità* moderne perseguono il "sogno di una società trasparente, visibile e leggibile in ciascuna delle sue parti", eliminando le zone d'oscurità create dal potere governativo[42].

Internet ha portato una maggiore trasparenza negli affari governativi. Tuttavia, ha anche reso gran parte della società trasparente a favore dei governi e delle aziende. La partecipazione online ha ampliato i confini della visibilità nel cyberspazio, sfidando la concezione tradizionale di intimità. Le piattaforme social hanno attivamente incoraggiato la partecipazione a questi ambienti di sorveglianza online. Promuovono l'idea che la sorveglianza sia positiva e auspicabile, nel tentativo di evitare la regolamentazione[43].

L'automazione, specialmente attraverso le tecnologie di *Machine Learning*, ha contribuito all'estensione della sorveglianza. Gli algoritmi sono centrali in questo processo di automazione e vanno considerati come parte dei "sistemi decisionali automatizzati", che combinano persone e codici computazionali in dinamiche complesse. Questi sistemi non sono neutri ma rappresentano forme di potere algoritmico e computazionale basate sulla sorveglianza[44]. In conclusione, la vigilanza basata sulla sorveglianza ha reso sempre più visibili gli aspetti della vita sociale privata attraverso Internet, influenzando il modo in cui le persone si autoregolano e interagiscono online.

Io sostengo che il controllo algoritmico, pur implicando sia sorveglianza sia disciplina, non dipende dal panottismo come meccanismo di potere. Nel potere algoritmico, la visibilità consente ancora l'esercizio del potere: la maggiore capacità di "vedere" i comportamenti e le comunicazioni apparentemente private degli individui consente alle piattaforme di estendere la loro portata sulla vita di tutti i giorni. Ma, come altre forme di iper-vigilanza algoritmica, il potere algoritmico non sarebbe panottico. Piuttosto, a causa della maggiore capacità di vedere, rappresenterebbe una forma di sorveglianza più ampia e totale. Potenzialmente ed ex ante, tutte, o sostanzialmente tutte, le comunicazioni su una piattaforma potrebbero di fatto essere sorvegliate. Non è necessario indurre incertezza nei soggetti della sorveglianza quando le moderne tecnologie di comunicazione, archiviazione ed elaborazione dei dati consentono ai sistemi di apprendimento automatico di spostare tali soggetti dall'essere permanentemente visibili all'essere permanentemente osservati[45]. Secondo Deleuze, il declino del panottismo nelle società occidentali ha fatto sì che queste si allontanassero sempre più dalle forme disciplinari di potere

[41] S. Zuboff, *Big other: surveillance capitalism and the prospects of an information civilization*, in "Journal of information technology*",* 30(1), 2015, pp. 75 ss.

[42] M. Foucault, *The History of Sexuality, Volume I: An Introduction*, New York: Vintage Press, 1980; trad. it. *La volontà di sapere*, Vol. 1, Milano, Feltrinelli, 2001.

[43] J.E. Cohen, *The surveillance-innovation complex: the irony of the participatory turn*, in D. Barney et al. (Eds.), *The Participatory Condition in the Digital Age*, Minneapolis, University of Minnesota Press, 2016.

[44] T. Gillespie, *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*, New Haven, Yale University Press, 2018.

[45] A. Lembke, *L'era della dopamina: Come mantenere l'equilibrio nella società del "tutto e subito"*, Milano, ROI Edizioni, 2022.

richieste da Foucault, diventando invece quelle che Deleuze chiama "società di controllo"[46]. Per Deleuze, il passaggio a una società di controllo significava meno confini rigidi attorno a ciò che si poteva e non si poteva fare. Per la maggior parte, gli individui sarebbero liberi di vivere la propria vita. Piuttosto che strutture fisse (fisiche o di altro tipo) intese a disciplinare gli individui in quanto soggetti principalmente fisici, le società di controllo adotterebbero mezzi flessibili, malleabili e variabili per modulare il comportamento. Attraverso queste strutture più flessibili, gli individui non sono soggetti al potere come un tutto unitario, ma sono invece un "dividuale" astratto[47], suddivisi in parti componenti – punti dati che descrivono interessi, preferenze, comportamenti e così via – che diventano essi stessi il luogo di controllo. L'individuo è ridotto ad un soggetto umano fisicamente incarnato che è infinitamente divisibile e riducibile a rappresentazioni di dati attraverso le moderne tecnologie di controllo, come i sistemi basati su computer[48]. Nonostante la loro architettura binaria, i computer possono produrre output ampliativi, variabili e predittivi per modulare il comportamento in base a ciò che è coinvolto e a ciò che è richiesto[49]. Nella società digitale, il potere non è tanto una questione di imporre vincoli ai cittadini quanto di restituire cittadini capaci di sopportare una sorta di libertà regolamentata: l'autonomia non è l'antitesi del potere, ma un termine chiave del suo esercizio, tanto più che la maggior parte degli individui non sono semplicemente soggetti del potere ma svolgono un ruolo attivo nei loro interventi[50]. Gli algoritmi non forniscono barriere rigide che impediscono agli individui di parlare liberamente (sebbene le piattaforme possano ovviamente imporre sospensioni e divieti agli utenti per violazioni gravi o ripetute attraverso i loro altri processi di moderazione). Ciò che, in definitiva, decide se una determinata comunicazione sarà consentita o soppressa è il giudizio dell'algoritmo su ciò che viene detto in quella comunicazione. In effetti, le politiche di moderazione più interventiste portano gli utenti ad autocensurarsi in misura maggiore, influenzando in modo significativo la discussione[51].

Non è irragionevole immaginare che, di fronte alla governamentalità algoritmica, molti utenti delle piattaforme social possano interiorizzare i confini percepiti dell'accettabilità e iniziare ad applicare questi confini alle proprie comunicazioni. Di fatto, questo li renderebbe autodisciplinati e modellerebbe le loro comunicazioni sui desideri dei grandi player del digitale. Attraverso la governamentalità algoritmica, il potere normativo delle piattaforme social assume una forma capillare. Questo potere si basa sulla sorveglianza, che permette alle piattaforme di monitorare le attività degli utenti e di modulare i contenuti in base alle loro preferenze.

[46] G. Deleuze, *Postscript on the Societies of Control* (1992), in D. Wilson, C. Norris (Eds.), *Surveillance, crime and social control*, London, Routledge, 2017, pp. 35 ss.

[47] A. Rouvroy, *The end(s) of critique: data-behaviourism versus due-process*, in M. Hildebrandt, E. De Vries (Eds.), *Privacy, Due Process and the Computational Turn. Philosophers of Law Meet Philosophers of Technology*. London, Routledge, 2013, pp. 143 ss.

[48] J. Cheney-Lippold, *We Are Data*, New York, New York University Press, 2017.

[49] L. Magnani, *Ingegnerie della conoscenza*. *Introduzione alla filosofia computazionale*, Milano, Marcos y Marcos, 1997.

[50] M. Dean, *Governmentality: Power and Rule in Modern Society*, London, Sage, 1999.

[51] R. Clark-Parsons, *Building a digital girl army: The cultivation of feminist safe spaces online*, in "New Media & Society", 20, 2018, pp. 2125 ss.

4. La privatizzazione algoritmica: "Algorithm is Law"

La privatizzazione algoritmica si manifesta come una modalità di controllo più attiva e interventista rispetto a quella che potrebbe essere ottenuta esclusivamente dagli esseri umani o attraverso sistemi non algoritmici. L'ordinamento privato opera in funzione del potere normativo delle piattaforme social in molteplici modi, indipendentemente dal fatto che tale potere sia esercitato direttamente dagli esseri umani o da algoritmi per loro conto. Ai termini di servizio, ad esempio, è stato riconosciuto un potere normativo simile a quello della legge[52]. Le piattaforme determinano i propri termini di servizio, apportando le modifiche che ritengono necessarie in qualsiasi momento. Oltre ai termini di servizio, le piattaforme di social media possono alterare i propri algoritmi per esercitare un controllo sulla diffusione e sull'amplificazione dei contenuti attraverso sistemi di personalizzazione, cercando di stimolare il coinvolgimento degli utenti e costruire quote di mercato, con conseguenze sempre più negative per la società[53].

Attraverso la vigilanza algoritmica, le piattaforme di social media possono impegnarsi in una forma di ordinamento privato più attiva e interventista di quanto sarebbe stato altrimenti possibile. Non tutta la moderazione sarà intrapresa esclusivamente per volontà delle piattaforme, ma anche laddove un certo controllo è imposto o incoraggiato dalla legge o dai regolamenti (per reprimere attività illegali come l'incitamento all'odio, ad esempio, o, negli stati autoritari, per ragioni politiche), è probabile che siano le stesse piattaforme social a essere responsabili dell'attuazione di tali requisiti, dello sviluppo di sistemi di sorveglianza e identificazione delle comunicazioni indesiderate e dell'attuazione della censura secondo le relative logiche. Le piattaforme potrebbero anche voler andare oltre i governi nel controllare le comunicazioni effettuate sulla loro piattaforma. Come discusso in precedenza, la capacità di farlo deriva dalle capacità dei sistemi algoritmici: disposizioni dinamiche di persone e codice computazionale. Il codice è stato da tempo riconosciuto come un sistema che fornisce una forma di potere normativo.

Lessig ha dimostrato come il codice, in maniera analoga all'architettura, stabilisca norme e confini. Sostiene infatti che, attraverso i suoi effetti architettonici, il codice agisca negli spazi virtuali come una vera e propria legge, offrendo una forma di controllo più passiva che facilita alcuni comportamenti e ne limita altri.

In questa forma di controllo, raramente si incontrano barriere rigide. Il comportamento viene modellato, influenzato e diretto principalmente attraverso il design, le funzionalità e le offerte di una piattaforma.

Lessig considerava l'architettura tecnica del web come il più grande protettore della libertà di parola. Affermava che il codice del web, grazie alla sua decentralizzazione, al relativo anonimato e alla mancanza di sistemi per identificare i contenuti, potesse prevenire la censura e fornire un Primo Emendamento globale. Inoltre, riteneva che il mercato, insieme al codice del web, potesse proteggere la libertà di espressione online[54]. La bassa barriera all'ingresso per i blog (in particolare) e altri media online permetteva a chiunque di presentare le proprie idee.

[52] M. Shapiro, *The Globalization of Law*, in "Indiana Journal of Global Legal Studies", 1(1), 1993, pp. 37 ss.

[53] H.M. Malik *et al*., *Social harms in an algorithmic context*, in "Justice, Power and Resistance", 5(3), 2022, pp. 193 ss.

[54] L. Lessig, *Code: Version 2.0*. http://codev2.cc/download+remix; 2006, pp. 236-237.

Già a metà degli anni Duemila, però, erano stati gettati i semi di un futuro molto diverso. La centralizzazione del web attorno a una manciata di aziende nel decennio successivo – la c.d. "cinta aperta" di internet – e il conseguente declino dei blog e di altre forme di comunicazione hanno cambiato radicalmente le condizioni descritte da Lessig (anche se, ai margini, esistono ancora mezzi alternativi di comunicazione).

Lo sviluppo da parte di queste aziende di sistemi più sofisticati per identificare ed eliminare attivamente i contenuti indica un cambiamento più fondamentale nel ruolo del codice nel controllo del comportamento. Si tratta di un avvertimento: il web sta venendo ricostruito per diventare un perfetto strumento di controllo.

Il codice del web, cioè la sua "architettura", potrebbe, in determinate circostanze, agire passivamente per prevenire la censura e favorire la libera espressione. Nondimeno, può anche diventare un mezzo di controllo del comportamento e della comunicazione. In quest'ultimo caso, ritengo che il codice incorporato nei sistemi algoritmici offra la possibilità a tali sistemi di essere difensori più attivi delle norme e dei comportamenti di quanto persino Lessig avesse previsto attraverso le caratteristiche più passive dell'architettura del codice (secondo il suo fortunato mantra "Code is Law"); i sistemi algoritmici possono effettivamente fungere da legge e forze dell'ordine contemporaneamente (secondo un diverso e nuovo mantra che chiamo "Algorithm is Law"). Questo si manifesta nell'uso dei sistemi di raccomandazione per personalizzare algoritmicamente i feed di contenuti, permettendo alle piattaforme di plasmare attivamente l'ambiente informativo presentato agli utenti e di promuovere o declassare specifici tipi di contenuti senza necessariamente rimuoverli o limitarne l'accesso[55].

Quando integrati nei processi per sopprimere o consentire attivamente le comunicazioni durante il caricamento, il livello di controllo esercitato sulle comunicazioni dal codice porta le piattaforme ancora più lontano da quanto Lessig avesse previsto. Questo tipo di controllo rimane in linea con la visione di Deleuze: raramente a un individuo viene impedito completamente di parlare; piuttosto gli viene impedito di esprimere determinati concetti, magari solo a certe persone o in determinati contesti, secondo il giudizio dell'algoritmo. Gli algoritmi svolgono un ruolo significativo nell'ordinamento privato attivo, combinando un potere funzionale (rilevamento e soppressione delle comunicazioni) con un potere normativo (applicazione delle regole e degli standard della piattaforma), stabilendo e mantenendo i confini del discorso accettabile online attraverso una forma di vigilanza attiva che implica una sorveglianza totale della comunicazione e del comportamento[56].

L'architettura informatica delle piattaforme di social networking determina una *de-medializzazione* della comunicazione: ciascuno produce e diffonde informazioni, sicché si evidenzia una tensione continua tra pratiche di esibizione e forme di intimità, un intreccio perenne tra spazi *online* e spazi *offline* all'interno di un *frame* complessivo che trova nella realtà (mediata o non mediata) le sue pratiche, le sue rappresentazioni e le sue conseguenze. Le persone vivono

[55] J. Danaher, *The Threat of Algocracy: Reality, Resistance and Accommodation*, in "Philosophy & Technology", 29, 2016, pp. 245 ss.

[56] M. Elbers, S. Navas (Eds.), *Algorithms and Law*. Cambridge (MA), Cambridge University Press, 2020.

questa doppia abitanza *online/offline*, cioè uno stato in cui si articola una sorta di *intimità digitale* dove la sperimentazione della relazione produce un vicinato digitale senza necessità di profondità relazionale. È uno stato di difficile gestione emotiva e affettiva che può esporre i minori a quella che Goffman definirebbe "perdita della faccia" non possedendo una completa consapevolezza che lo spazio digitale vede la convergenza del concreto e del virtuale in modo circolare, teso tra forme di intimità e pratiche di esibizione. La rete, infatti, pur non permettendo la presenza fisica, veicola informazioni, pulsioni, affetti e definizioni immediatamente attualizzate nelle pratiche fisiche: dalle posizioni sessuali imparate attraverso la pornografia sino alla definizione di ciò che è normale e anormale in rapporto alla sfera intima[57].

I limiti dei nuovi media digitali non fanno soltanto apparire le persone un po' più fredde, irascibili e intolleranti: *online* è facile essere realmente meno inclini a comportarsi in modo civile ed educato, almeno nella misura in cui richiederebbero le norme sociali. Una perdita di innocenza accompagna quindi l'espansione di una rete.

L'interfaccia con la macchina può amplificare una indifferenza amorale per le relazioni umane. Senza incontrare gli altri fisicamente, la nostra etica viene meno. Le persone non si osservano più tra loro ma diventano *voyeurs*. Senza la presenza umana diretta, senza la comunicazione faccia a faccia che stabilisce i confini della fiducia, la partecipazione diventa opzionale: mantenere il distacco pur partecipando può ridurre la fiducia e diffondere un cinico anonimato.

Ad esempio, l'uso generale delle tecnologie d'identificazione su Internet accrescerebbe la regolabilità del comportamento nel cyberspazio: quest'opzione tecnica, implementabile dai governi, renderebbe impossibile qualsiasi raccolta e trasmissione di dati personali d'identificazione sull'utente.

Le regole dello spazio reale – qui sta il punto decisivo della questione – dipendono da certe caratteristiche di *design*. Nello spazio reale l'età è un fatto immediatamente conoscibile: ovviamente un ragazzo potrebbe cercare di dissimularla, ma generalmente ciò non accade; infatti, all'adulto che vende o tratta pornografia è nota la minore età del ragazzo. Nello spazio reale l'autenticazione di sé consente facilmente di creare zone che rendono *off-limits* i contenuti osceni dell'espressione.

Nel cyberspazio, invece, l'età non è immediatamente conoscibile. Quand'anche le stesse restrizioni di mercato, nonché le stesse leggi e norme sociali, trovassero applicazione al cyberspazio, ogni tentativo di istituire delle zone *off-limits* per la pornografia si scontrerebbe con la difficoltà concreta di accertare l'età. Per un sito che accetta il traffico utente, ogni richiesta è identica alle altre: l'architettura fondamentale del cyberspazio garantisce l'invisibilità alle caratteristiche dell'utente.

L'unica soluzione che consenta di identificare l'età parrebbe essere la modifica del *code* della Rete per consentire la trasmissibilità delle informazioni relative all'età *dell'user* e per rendere tracciabile l'anonimato. È pur vero che, allo stato attuale, non c'è un rapporto necessario

[57] Il processo di addomesticamento della pornografia (*domestication of pornography*) consiste nell'assimilare le pratiche e le tecniche sessuali esplicite ed estreme entro i significati propri della vita quotidiana e quindi del contesto sociale e relazionale in cui si è inseriti.

tra un terminale (avente un dato indirizzo IP) e la persona; i governi, però, potrebbero intervenire per facilitare l'uso delle tecnologie di identificazione e di autenticazione degli utenti sul web.

Le tutele sul web sono dunque possibili, a condizione, però, d'imporre un giudizio relativo ai soggetti che dovrebbero avere accesso a determinati contenuti, cui verrebbero sottoposti anche coloro che compongono il *code* informatico; in tal modo, anche le architetture del cyberspazio sarebbero disegnate in conformità alle regole statali.

Un esempio della forma più attiva e interventista di ordinamento privato abilitata dagli algoritmi si manifesta nello sviluppo nel tempo di diversi metodi digitali di protezione della proprietà intellettuale. L'ascesa della gestione dei diritti digitali ("DRM") ha rafforzato gli standard IP, ma in modo relativamente passivo. Ad esempio, se il contenuto non era fornito con la chiave digitale corretta o era incompatibile con il sistema DRM utilizzato dal software o dalla piattaforma in questione, non era possibile riprodurlo; non veniva effettuata né un'analisi né un'applicazione attiva basata sul contenuto. Lo sviluppo del sistema ContentID di YouTube, un processo algoritmico che controlla attivamente tutti i video caricati per individuare materiale potenzialmente in violazione della proprietà intellettuale, rappresenta una forma più attiva di intervento basato su codice[58]; di fatto, gli standard IP di YouTube diventano legge sulla sua piattaforma, applicati attivamente da ContentID. Per analogia con altre aree di regolamentazione, se i DRM si limitano a verificare la documentazione, ContentID invece esamina il contenuto.

Attraverso il controllo algoritmico, il codice delle piattaforme social non solo vincola o facilita determinati comportamenti attraverso effetti architettonici, ma può anche analizzare il contenuto e intervenire attivamente per sopprimerlo (ex ante) al momento del caricamento. Il controllo algoritmico, come parte della vigilanza algoritmica, può essere considerata una forma di regolazione algoritmica; in particolare, è una manifestazione di ciò che Hildebrandt definisce "regolamentazione guidata da codici" per descrivere sistemi in cui il sistema stesso cerca di modificare il comportamento[59]. In questo contesto, le piattaforme social potrebbero far rispettare più attivamente i propri standard di comunicazione accettabile, che funzionano effettivamente come legge su tali piattaforme. La capacità di farlo porta le piattaforme oltre ciò che potrebbero ragionevolmente ottenere utilizzando revisori umani. La vigilanza algoritmica - attraverso la diffusa portata di questo potere che si estende alle conversazioni private e quotidiane, tramite l'intervento attivo delle piattaforme - potrebbe fornire una sorta di potere di regolamentazione privato sulle strutture interattive.

5. Forme escludenti e stereotipi del mercato algoritmico

La funzione strategica del dispositivo sulle piattaforme social dovrebbe essere principalmente interpretata in relazione alle priorità commerciali: entrate, posizionamento di mercato e

[58] J. Cobbe, *Algorithmic Censorship by Social Platforms: Power and Resistance*, in "Philosophy & Technology", 34, 2021, pp. 739 ss.

[59] M. Hildebrandt, *Algorithmic regulation and the rule of law*, in "Philosophical Transactions of the Royal Society", 2018, pp. 1 ss.

profitto soprattutto. È importante notare che questi sistemi algoritmici non sono neutrali né imparziali; essi riflettono le priorità e gli obiettivi dei loro progettisti, implementatori e utenti, influenzando così i cambiamenti nelle dinamiche di potere e nelle condizioni strutturali. Attraverso il controllo algoritmico, le piattaforme social possono plasmare in modo più incisivo i comportamenti sociali conformemente alle priorità commerciali.

Sebbene le piattaforme social siano diventate luoghi sempre più cruciali per il dibattito politico, le relazioni interpersonali, la comunità e la solidarietà, la commercializzazione delle comunicazioni pubbliche e private e delle conversazioni quotidiane da parte di queste piattaforme può avere effetti negativi sulla loro capacità di svolgere appieno questo ruolo. Poiché le piattaforme social gestite per fini commerciali tendono a privilegiare considerazioni economiche rispetto ad altre, spesso non pongono la libertà di espressione come priorità né dedicano sufficiente attenzione al ruolo sociale che svolgono come mediatori delle comunicazioni pubbliche e private. Inoltre, non promuovono in genere coerenza, equità o trasparenza nelle loro politiche di moderazione[60]. A causa delle loro priorità commerciali orientate alla crescita, al dominio del mercato e al profitto, le piattaforme social tendono a cercare un vasto pubblico *mainstream* per soddisfare gli inserzionisti e i politici e per evitare una regolamentazione potenzialmente costosa. Di conseguenza, spesso non offrono spazio sufficiente agli emarginati, alle minoranze o a coloro con opinioni non convenzionali[61]. Inoltre, inchieste giornalistiche hanno evidenziato come il perseguimento di obiettivi commerciali abbia portato alcune piattaforme a escludere le lavoratrici del sesso e a emarginare donne e persone LGBTQ+ attraverso la rimozione o la limitazione delle loro comunicazioni[62].

La natura discriminatoria delle piattaforme social, derivante dagli interessi commerciali, potrebbe essere accentuata o amplificata dalle limitazioni degli algoritmi utilizzati. La parzialità rappresenta una sfida significativa per gli algoritmi di censura in generale. L'identificazione e la rimozione automatica dell'incitamento all'odio sono complesse e possono portare alla censura delle vittime potenziali; ad esempio, un'analisi sull'incitamento all'odio ha rivelato che i tweet degli utenti afroamericani erano più spesso etichettati come offensivi rispetto ad altri[63]. Queste limitazioni e pregiudizi possono portare a una maggiore censura delle comunicazioni dei gruppi emarginati. La percezione degli utenti riguardo ai pregiudizi negli algoritmi di censura, insieme alla natura escludente delle politiche commerciali delle piattaforme, potrebbe contribuire a un effetto disciplinare della censura algoritmica, favorendo l'autocensura e creando un "effetto bandwagon" in cui le opinioni emarginate vengono sopite percependo che non siano ben accette in questi contesti commerciali[64].

[60] L. Wright, *Automated Platform Governance Through Visibility and Scale: On the Transformational Power of AutoModerator*, in "Social Media + Society", 2022, pp. 1 ss.

[61] E.A. Vogel et al., *Problematic Social Media Use in Sexual and Gender Minority Young Adults: Observational Study*, in "JMIR Ment Health.", 8(5), 2021, e23688.

[62] B. Dhiman, *Impact of Social Media Platforms on LGBTQA Community: A Critical Review*. 2023. Available at SSRN: https://ssrn.com/abstract=4410280; consultato in data 6 febbraio 2024.

[63] F. Poletto et al., *Resources and benchmark corpora for hate speech detection: a systematic review*, in "Language Resources and Evaluation", 55, 2021, pp. 477 ss.

[64] T. de Groot *et al.*, *Learning in and about a filtered universe: young people's awareness and control of algorithms in social media*, in "Learning, Media and Technology", 48(4), 2023, pp. 701 ss.

Sebbene gli inserzionisti e la minaccia di regolamentazione possano influenzare i cambiamenti nelle politiche dei social media, queste piattaforme dimostrano uno scarso interesse a considerare sistematicamente le opinioni degli utenti su ciò che è accettabile.

I processi di moderazione rimangono opachi e inaccessibili. In generale, gli utenti non dispongono di mezzi formali per influenzare direttamente i limiti del discorso accettabile. Le piattaforme social spesso adottano meccanismi di revisione irrispettosi anche verso i loro stessi processi di moderazione umana, rifiutandosi frequentemente di fornire informazioni chiare sulle regole e la loro applicazione.

L'evoluzione delle policies avviene spesso attraverso decisioni unilaterali prese in risposta a campagne prolungate e a un'ampia indignazione, anziché tramite processi democratici e responsabili per definire i confini del discorso accettabile. È importante notare che tali cambiamenti politici sono a discrezione delle piattaforme stesse, non il risultato di processi trasparenti, responsabili o democratici. Le piattaforme social tendono a prioritizzare gli interessi degli azionisti e la ricerca del profitto, anziché quelli degli utenti o della società in generale.

La funzione strategica principale delle piattaforme social non è necessariamente il libero scambio di idee, la condivisione di informazioni o la costruzione di comunità, bensì la generazione di profitti, la posizione sul mercato e il vantaggio per le stesse piattaforme social.

Attraverso la vigilanza algoritmica, le piattaforme social assumono unilateralmente il ruolo di mediatori e moderatori attivi delle comunicazioni online: un'azione altrimenti impraticabile senza altri meccanismi per influenzare l'ambiente informativo o moderare le comunicazioni. Questo potere normativo permette loro di identificare e sopprimere l'emergere di discorsi e di pensieri alternativi ritenuti commercialmente svantaggiosi, decidendo di eliminare automaticamente comunicazioni lecite ma sgradite, indesiderate o non mainstream per proteggere i propri flussi di entrate. Di conseguenza, la partecipazione a conversazioni ordinarie e a forum di discussione socialmente rilevanti diventano sempre più soggetta alle priorità aziendali. L'introduzione di sistemi algoritmici di censura modifica e commercializza ulteriormente le condizioni strutturali della discussione, del discorso e della connessione interpersonale, consentendo alle piattaforme di imporre limiti commercialmente determinati al discorso accettabile in modo più efficace. Il risultato è la creazione di piattaforme social omologanti e asettiche, che favoriscono comunicazioni commercialmente accettabili escludendo comunità e voci alternative. Nonostante le piattaforme social enfatizzino i benefici della comunicazione, della connessione e della condivisione di esperienze e di idee, la commercializzazione delle comunicazioni attraverso la vigilanza algoritmica rischia di compromettere significativamente la loro capacità di offrire spazi realmente inclusivi.

6. Il governo algoritmico della violenza digitale di genere

Il mondo digitale si è trasformato in un ambiente favorevole alla violenza di genere, con la mancanza di spazi inclusivi che hanno favorito la diffusione rapida di questa forma di violenza.

L'implementazione degli algoritmi ha condotto al monitoraggio dei contenuti considerati inadeguati o offensivi, ma ha altresì determinato l'oscuramento delle voci femminili e delle minoranze, agevolando la proliferazione di contenuti misogini e violenti. Tale disparità algoritmica ha represso la libertà di espressione.

La carenza di spazi inclusivi e sicuri nel mondo digitale ha reso le donne e le persone LGBTQ+ particolarmente vulnerabili alla violenza di genere. L'assenza di regole adeguate ha favorito la creazione di un ambiente digitale tossico, che facilita la diffusione di molestie, minacce e abusi. I legami tra violenza di genere e tecnologia non sono nuovi, ma solo recentemente si è compreso appieno come le tecnologie digitali possano essere ambienti oppressivi.

È essenziale comprendere come gli autori di reati possano sfruttare la tecnologia digitale per esercitare controllo sulle loro vittime, evidenziando la necessità di affrontare in modo approfondito le complessità della violenza di genere nel contesto digitale[65].

Le tecnologie digitali e la violenza di genere si intrecciano a livello interpersonale e strutturale. La violenza di genere a livello individuale riflette e rafforza dinamiche strutturali come il sessismo e il razzismo[66]. Con l'avvento delle tecnologie digitali, le questioni legate alla violenza strutturale diventano sempre più cruciali. La violenza strutturale è nella architettura digitale stessa e si manifesta come disuguaglianza di potere e di opportunità di vita.

Le tecnologie digitali influenzano le nostre interazioni sociali pubbliche e private, creando nuovi modi di comunicare con partner, familiari, amici e istituzioni sociali[67]. Nuove tecnologie offrono agli autori di reati maggiori possibilità di perseguitare, isolare e controllare le loro vittime.

Oltre alle forme dirette di violenza di genere tecnologica, si sono sviluppate piattaforme online misogine, razziste e discriminatorie, che favoriscono visioni stereotipate e dispregiative[68]. In questo contesto online non regolamentato, gruppi emarginati sono particolarmente vulnerabili alle molestie e agli attacchi online.

Nonostante i rischi, le tecnologie digitali offrono anche opportunità per l'attivismo sociale e la resistenza. Gli ambienti digitali consentono la creazione di comunità diverse e distanti geograficamente, supportando i "resistenti" attraverso spazi autentici in cui sentirsi ascoltati. Campagne come #metoo hanno dimostrato il potenziale dell'ambiente digitale nel democratizzare l'accesso alla voce e sfidare l'esclusione.

L'attivismo digitale rappresenta una parte importante del femminismo contemporaneo, ma è essenziale collegarlo ai movimenti sul campo per garantire un impatto reale anche per coloro che non hanno accesso digitale, creando forme di solidarietà che superano le divisioni nazionali.

Nondimeno, il cyberfemminismo non può essere considerato la soluzione universale per la lotta alla disuguaglianza di genere, poiché le disparità digitali creano una frattura nell'idea di un movimento cyberfemminista universale. Questo mette in evidenza la necessità che l'attivismo

[65] C. Barter, S. Koulu, *Special issue: Digital technologies and gender based violence – mechanisms for oppression, activism and recovery*, in "Journal of Gender-Based Violence", 5(3), 2021, pp. 367 ss.

[66] A. Kleinman, *The Violence of Everyday Life: The multiple forms and dynamics of social violence*, in V. Das (ed) *Violence and Subjectivity*, Los Angeles, University of California Press, 2000, pp. 226-241.

[67] S. Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Other*, New York, Basic Books, 2011.

[68] J. Leung, *Shortcuts and Shortfalls in Meta's Content Moderation Practices*, in "Comparative Law and Language", 1(2), pp. 55 ss.

online contro la violenza di genere sia strettamente collegato ai movimenti comunitari di resistenza sul campo per includere le donne e le ragazze prive di accesso digitale[69].

Le cyberfemministe, ispirate dal lavoro di Haraway[70], immaginavano un futuro in cui la tecnologia avrebbe eliminato i vincoli di genere e altri attributi corporei, trasformando il cyberspazio in un luogo di libertà e emancipazione. Grazie all'anonimato offerto dalla rete, queste donne hanno visto nell'uso del computer un modo per riappropriarsi della tecnologia, considerandola come uno strumento di empowerment per le donne e altri generi non egemoni[71]. Le nuove tecnologie hanno contribuito a smantellare le costruzioni tradizionali di genere e sessualità, aprendo spazi per identità fluide e multiple al di fuori dei limiti imposti dalla realtà fisica[72]. Altre cyberfemministe hanno sostenuto che il cyberspazio ha reso più sfumato il confine tra umano e macchina[73], offrendo opportunità per liberare le donne dai binari rigidi uomo/donna e tecnologia/natura che le hanno a lungo oppresse. Questa visione ha permesso la creazione di identità e relazioni umane al di là delle categorie di genere tradizionali, promuovendo una maggiore diversità e fluidità nell'espressione dell'identità[74].

Le tecnologie digitali sono spesso considerate come spazi per la costruzione di identità "flessibili" o "fluide", che sfidano i tradizionali dualismi di genere e le gerarchie di potere. Ciò nonostante, contemporaneamente possono anche favorire la diffusione di norme di genere più tradizionali. Questa visione contrastante della tecnologia come liberatoria o dannosa è supportata da numerose studiose femministe della tecnologia[75].

È cruciale riconoscere che le donne sono attivamente coinvolte nell'innovazione tecnologica e ne traggono benefici, evitando di dipingere le donne esclusivamente come vittime passive della tecnologia. L'obiettivo qui è mettere in luce gli impatti negativi legati all'interazione, all'esclusione e alla violenza tecnologica. Inoltre, ci si propone di esaminare gli effetti delle molestie sessuali e della violenza facilitate dalla tecnologia e come vengono affrontati in ambito giuridico e politico.

Si presenta una sfida unica: se da un lato le nuove tecnologie offrono la possibilità di superare i limiti del corpo fisico, dall'altro il dualismo tra corpo e mente può complicare la comprensione degli impatti di tali danni[76].

[69] M. Desai, *Gender and the Politics of Possibilities: Rethinking Globalization*, Washington (DC), Rowman & Littlefield Publishers, 2009.

[70] D. Haraway, *A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980's*, in "Australian Feminist Studies", 2(4), 1987, pp. 1 ss.

[71] D. Lupton, *Sociologia digitale*, Milano-Torino, Pearson, 2018, pp. 99 ss.

[72] J. Wajcman, *Technofeminism*, Cambridge (UK), Oxford, Polity Press, 2004.

[73] S. Plant, *Zeroes + Ones: Digital Women and the New Technocultur*e, London, Doubleday, 1997; trad. it. *Zero, Uno. Donne digitali e tecnocultura*, Milano, LUISS University Press, 2021.

[74] R. Braidotti, *Cyberfeminism with a difference*, in M.A. Peters, M. Olssen, C. Lankshear (Eds.), *Futures of critical theory: Dreams of difference*, 1996, pp. 239 ss.

[75] D.C. Parry et al., *Digital Dilemmas: Transforming Gender Identities and Power Relations in Everyday Life*, in D.C. Parry, C.W. Johnson, S. Fullagar (Eds.), *Digital Dilemmas*, Cham, Palgrave Macmillan, 2019.

[76] E. Grosz, *Volatile Bodies: Toward a Corporeal Feminism*, Bloomington, Indiana University Press, 1994.

Le tecnologie digitali sono impiegate per offrire supporto sociale e psicologico, sebbene possano essere criticati per essere impersonali e distanti, per alcuni rappresentano un mezzo accessibile che non è condizionato dagli obblighi familiari e lavorativi. Ma, come precedentemente sottolineato, l'accesso alla tecnologia digitale non è uniformemente distribuito e può dipendere da vari fattori come l'accesso alle infrastrutture digitali, la disponibilità di *digital devices*, le disabilità e l'alfabetizzazione digitale. I problemi di accesso possono quindi accentuare le disuguaglianze presenti in molte forme di violenza di genere.

L'aumento dell'utilizzo delle tecnologie digitali, sia nel favorire che nel contrastare la violenza, costituisce una sfida per il diritto e i sistemi giuridici. Il cyberbullismo e lo stalking online alterano la natura geografica, spaziale e temporale dell'abuso, generando questioni intricate legate alla giurisdizione e alla legalità. L'ampio impatto delle tecnologie digitali può mettere alla prova le istituzioni giuridici poiché la legge tradizionalmente si basa su presupposti che circoscrivono i reati territorialmente, nel tempo e nello spazio, imputandoli a singoli individui; il rapporto tra il pensiero giuridico e le tecnologie digitali è strettamente correlato ai valori e alle decisioni dei programmatori tecnologici[77].

Inoltre, le tecnologie digitali costringono la legislazione a rivalutare il concetto di privacy e sfera privata, riconsiderando ad esempio gli elettrodomestici smart e le apparecchiature di sorveglianza domestica come possibili strumenti di stalking. La sfida consiste nel combinare diversi approcci per garantire l'accesso alla giustizia, alla tutela giuridica e al pieno potenziale degli ambienti digitali.

7. Analizzare la violenza digitale di genere

La violenza digitale è un fenomeno in rapida espansione su Internet, caratterizzato da diverse pratiche: dalla diffusione non consensuale di immagini sessuali, alle minacce esplicite di violenza sessuale fino al furto di identità. Per molte donne, questo può significare la diffusione non autorizzata delle loro immagini sessuali come forma di controllo sul proprio corpo. Allo stesso tempo, le donne che protestano contro l'impunità per la violenza di genere rischiano di ricevere minacce di violenza sessuale online per silenziarle. Questi esempi sono collegati a due concetti presenti nella letteratura sulla violenza di genere: la violenza generale contro le donne per erodere la coesione sociale e rafforzare la subordinazione femminile[78] e la violenza contro le donne impegnate in politica per escluderle dalla sfera politica[79].

Nonostante esista una vasta letteratura riguardante varie forme di delinquenza digitale, come il cyberbullismo e la cyberpornografia[80], c'è stata scarsa attenzione rivolta alla "violenza e molestie sessuali agevolate dalla tecnologia" ("Technology-facilitated Sexual Violence" –

[77] E. Maestri, *Lex Informatica e soft law. Le architetture normative del cyberspazio*, in P. Moro, C. Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, FrancoAngeli, pp. 157 ss.

[78] M.L. Krook, *Violence against women in politics*, Berlin, Springer International Publishing, 2020.

[79] D. K. Cohen, S. M. Karim, *Does more equality for women mean less war? Rethinking sex and gender inequality and political violence*, in "International organization", 76(2), 2022, pp. 414 ss.

[80] N. Henry, A. Powell, *The dark side of the virtual world: Towards a digital sexual ethics. Preventing sexual violence: Interdisciplinary approaches to overcoming a rape culture*, London, Palgrave Macmillan, 2014, pp. 84 ss.

TFSV)[81]. Questo concetto denota comportamenti aggressivi di natura sessuale perpetrati contro le donne mediante l'utilizzo di nuove tecnologie. Le TFSV possono essere categorizzate in sei diverse modalità, tra cui la creazione e la diffusione non autorizzata di immagini a sfondo sessuale, l'utilizzo dei mezzi di trasporto per commettere violenza sessuale e lo stupro virtuale.

L'impiego delle nuove tecnologie come smartphone e social media è ampiamente diffuso nella società contemporanea, specialmente tra i giovani adulti, modificando il modo in cui le persone si collegano e interagiscono socialmente. La tecnologia ha rivoluzionato la comunicazione, consentendo una maggiore connettività e forme di interazione sociale innovative.

Le nuove tecnologie sono sfruttate per perpetuare disuguaglianze di genere sia antiche che nuove, oltre che per commettere atti criminali e comportamenti dannosi. La letteratura criminologica sul crimine informatico distingue tra crimini tradizionali adattati alla tecnologia (assistiti dalla tecnologia) e nuove forme di reato rese possibili solo grazie agli avanzamenti delle tecnologie digitali[82].

Alcuni studiosi argomentano che, sebbene alcune manifestazioni della criminalità virtuale siano nuove, la maggior parte dei crimini informatici differisce solo per il mezzo utilizzato. In contrasto, altri criminologi enfatizzano che le distinzioni tra criminalità online e offline sono sostanziali e qualitative[83]. Le tecnologie dell'informazione e della comunicazione agiscono come moltiplicatori di forze, permettendo impatti negativi su numerose vittime con relativamente minori sforzi da parte degli autori dei reati.

Nel panorama della criminalità informatica, il cyberspazio presenta elementi che amplificano la forza e l'impatto delle attività illegali rispetto alla criminalità tradizionale. Questi elementi includono il superamento delle barriere spazio-temporali, la connettività multipla che consente a un autore di colpire molteplici bersagli e l'anonimato online che agevola l'inganno e rende la regolamentazione più complessa. In sintesi, il cyberspazio offre numerosi obiettivi potenziali, incentivi per i trasgressori e sfide significative nella protezione e regolamentazione delle attività criminali online[84].

Benché la cybercriminalità abbia attirato molta attenzione all'interno degli studi criminologici[85], rimane una scarsità di lavori empirici e teorici che esplorano i danni digitali subiti in particolare dalle donne. Alcuni lavori riguardano le molestie sessuali e l'adescamento online[86], il

[81] N. Henry, A. Powell, *Embodied harms: Gender, shame, and technology-facilitated sexual violence*, in "Violence against women", 21(6), 2015, pp. 758 ss.

[82] A.C. Amato Mangiameli, G. Saraceni, *I* reati informatici*. Elementi di teoria generale e principali figure criminose*, Torino, Giappichelli, 2019.

[83] T. Holt, A. Bossler, *Cybercrime in progress: Theory and prevention of technology-enabled offenses*, London, Routledge, 2015.

[84] S. Hall, *Theorizing crime and deviance: A new perspective*, Thousand Oaks (CA), Sage Publishing, 2012.

[85] J. Clough, *Principles of cybercrime*, Cambridge (MA), Cambridge University Press, 2015.

[86] D. Chambers, *Social media and personal relationships: Online intimacies and networked friendship*, Berlin, Springer, 2013.

sexting non consensuale e il "revenge porn"[87], l'hate speech di genere[88] e lo stupro virtuale, in cui l'avatar di una persona (o la sua rappresentazione digitale) viene sottoposto a violenza sessuale simulata da altri avatar, più recentemente nel mondo virtuale tridimensionale del Metaverso.

Gli studi sull'impatto delle nuove tecnologie nella violenza sessuale contro le donne sono limitati, non documentando adeguatamente la diffusione di questi danni. Questa mancanza è sorprendente considerando i casi di alto profilo legati al sexting non consensuale e allo stupro virtuale. La scarsa attenzione di genere negli studi sulla criminalità informatica ha portato a una concezione insufficiente del danno digitale inflitto alle donne.

Inoltre, lo status della cosiddetta realtà virtuale è esso stesso oggetto di un ampio dibattito[89]. Gli ambienti virtuali come spazi liminali, luoghi sacri di trasformazione sociale e personale, né immaginari né reali, animati ma non vivi né morti, un regno soggettivo di immaginazione esteriorizzata dove gli eventi accadono in effetti ma non in realtà. Michael Benedikt definisce analogamente il cyberspazio come una realtà multidimensionale artificiale o virtuale, in rete e generata dal computer, dove gli oggetti visti o ascoltati non sono né fisici né necessariamente rappresentazioni di oggetti fisici ma sono – nella forma, nel carattere e nell'azione – costituiti da dati e da pura informazione[90]. Alcuni studiosi suggeriscono che i danni virtuali (online) non sono paragonabili a quelli del mondo reale (offline)[91]. Ad esempio il danno della violenza sessuale è profondamente legato alla carne dei corpi[92].

Al contrario, Gillian Youngs sostiene che dobbiamo pensare in termini socio-spaziali quanto geo-spaziali, dove socio-spaziale si riferisce agli spazi mediati tecnologicamente a cui possiamo accedere, lavorare e giocare, costruire relazioni e comunità, prefiggersi la comprensione, ecc.[93]. La rapida espansione dell'uso di Internet e di altre tecnologie di comunicazione ha portato a un cambiamento significativo, in cui le interazioni sociali non sono solo mediate dalla tecnologia, ma sempre più dipendenti da essa. Pertanto, le nostre comunicazioni e interazioni sociali nei mondi socio-spaziali o tecno-sociali possono diventare altrettanto o più importanti del contesto geo-spaziale.

Le categorie giuridiche tradizionali del diritto penale faticano ad affrontare i danni digitali o tecno-sociali. Come osserva Sheila Brown, il codice penale si basa sulla nozione di protezione del corpo da danni e violazioni dolose, richiedendo la presenza di individui incarnati per accertare la colpevolezza e applicare la punizione.

[87] K. Walker, E. Sleath, *A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media*, in "Aggression and violent behaviour", 36, 2017, pp. 9 ss.

[88] M.C. Nussbaum, *From disgust to humanity: Sexual orientation and constitutional law*, Oxford, Oxford University Press, 2010; trad. it. *Disgusto e umanità. L'orientamento sessuale di fronte alla legge*, Milano, Il Saggiatore, 2011.

[89] N. Henry, A. Powell, *The dark side of the virtual world: Towards a digital sexual ethics. Preventing sexual violence: Interdisciplinary approaches to overcoming a rape culture*, cit., pp. 84 ss.

[90] M. Benedikt (Ed.), *Cyberspace: First Steps*, Cambridge (MA), The Mit Press, 1991; trad. It. *Cyberspace: primi passi nella realtà virtuale*, Padova, F. Muzzio, 1993.

[91] M. Williams, *Virtually criminal: Crime, deviance and regulation online*, New York, Routledge, 2006.

[92] J. Wolfendale, *My avatar, my self: Virtual harm and attachment*, in "Ethics and information technology", 9, 2007, pp. 111 ss.

[93] G. Youngs, *Global political economy in the information age: Power and inequality*, London, Routledge, 2007.

La domanda cruciale diventa: il danno deve necessariamente essere inferto al corpo di un individuo per essere considerato tale? Oppure, come sostiene Brown, quanto deve essere incarnata la "reale" vittimizzazione?

I danni subiti nel cosiddetto mondo virtuale possono avere effetti reali, sia fisici che psicologici. Non sono affatto tangenziali, ma assumono un ruolo sempre più centrale nel modo in cui gli individui sperimentano e vivono la loro vita quotidiana.

I danni subiti dalle donne nello spazio socio-digitale possono avere un impatto sulla persona almeno pari a quello dei danni tradizionali che si verificano sul corpo fisico. Come afferma Brown, i pixel che circolano e si diffondono all'infinito influenzano le vite reali, generando umiliazioni e sofferenze umane concrete, e riproducendo e rafforzando relazioni reali di potere e sfruttamento[94].

Non è automatico che debba esistere una legge direttamente applicabile contro la violenza sessuale nella vita reale e i suoi equivalenti virtuali, come lo stupro virtuale. Al contrario, i danni digitali inflitti alle donne devono essere trattati come danni distinti, anche se la loro natura, estensione e frequenza richiedono ulteriori teorizzazioni e indagini per sviluppare rimedi giuridici praticabili ed adeguati. Tali danni devono essere valutati considerando anche il loro potenziale impatto.

Attualmente, vi sono pochi casi in cui danni virtuali o sessuali sono considerati seriamente come reati penali, fatta eccezione per l'adescamento e lo sfruttamento sessuale dei minori, il cyberbullismo e le molestie online. Un esempio significativo di questa sfida è il sexting, che consiste nell'invio di immagini sessuali attraverso mezzi digitali come telefoni cellulari, chat video online e social network. Il diritto penale si trova ad affrontare la diffusione di immagini sessuali non autorizzate in questo contesto.

Recentemente, l'attenzione si è concentrata sul sexting non consensuale, con particolare riguardo alla partecipazione delle ragazze e delle giovani donne, considerata sia la vittimizzazione sessuale sia la complicità nella produzione di pornografia infantile[95]. Molti Paesi hanno proposto leggi sul revenge porn o sul sexting per affrontare questi comportamenti e proteggere i minori.

Il sexting e la diffusione non autorizzata di immagini sessuali mettono in luce le criticità legislative quando non si adattano alle nuove tecnologie e possono danneggiare le vittime coinvolte. È cruciale considerare il danno causato alla vittima, violando la sua autonomia sessuale e provocando umiliazione o molestie[96].

In sintesi, il problema delle TFSV viene spesso associato alla protezione dei giovani dai pericoli online, ma è importante considerare anche le nuove forme di danni emergenti e la dimensione di genere di tali violazioni.

[94] S. Brown, *Integration by way of the criminology of hybrids*, in G. Barak (Ed.), *Criminology: An integrated approach*, Plymouth, Rowman & Littlefield, 2006.

[95] T. Crofts *et al.*, *Sexting and young people*, Berlin, Springer, 2016.

[96] A. Powell, *Sex, power and consent: Youth culture and the unwritten rules*, Melbourne, Cambridge University Press, 2010.

Le nuove tecnologie di comunicazione, come gli smartphone, i siti di social network e le applicazioni software, consentono la distribuzione di immagini e filmati sessuali in vasti spazi geografici. La tecnologia digitale crea un ambiente unico per la vergogna sociale. Ciò non implica necessariamente che il danno di un episodio sia uguale a quello dell'altro, ma piuttosto che il danno originario di una violazione, di una molestia o di un discorso di odio sia esacerbato dalla natura illimitata della vergogna e dell'umiliazione pubblica potenziale e perpetua. Le TFSV sollevano quindi seri interrogativi non solo su come rispondere adeguatamente a questi danni, ma anche su come inquadrarli e comprenderli.

Malgrado molti autori giudicano il mondo virtuale come una liberazione dalle costrizioni di genere del mondo fisico offline, sarebbe errato concludere che l'essere corporeo sia del tutto assente nel cyberspazio. In effetti, le TFSV potrebbero essere intese come danni di genere esplicitamente o implicitamente fissati sull'oggettivazione del corpo femminile. In altre parole, il corpo femminile, sia reale che immaginario, è inscritto, marcato e assoggettato[97].

Martha Nussbaum sostiene che questa oggettivazione comporta sempre il conferimento all'oggetto di un'identità viziata o stigmatizzata, cioè uno status compromesso. E aggiunge che oggettivare significa trattare come una mera cosa, come uno strumento per gli scopi dell'oggettivatore, come un'entità i cui sentimenti soggettivi non devono essere presi in considerazione, o i cui sentimenti, come la sua autonomia, possono essere deliberatamente violati[98].

Nussbaum afferma che l'oggettivazione misogina su Internet è profondamente legata alla punizione della vergogna. Questa oggettivazione è spesso condizionata dalla riduzione e dallo svilimento dell'oggetto a parti del corpo e all'aspetto fisico.

Il risentimento, spiegato da Nussbaum, è un'emozione reattiva ispirata dal sentimento di debolezza. L'obiettivo del risentimento è abbattere le persone e ottenere potere su di loro. La tecnologia incarna e amplifica il potere stesso; il potere di far circolare informazioni o testi a costo zero, in ogni angolo del mondo. L'anonimato e la complicità provvedono alla protezione necessaria per questo potere incontenibile, dove il corpo femminile, costruito come aberrante differenza sessuale, diventa il tramite per la gratificazione e l'oggettivazione sia nel mondo geospaziale sia in quello socio-spaziale. Ciò contrasta con l'ottimismo di Haraway secondo cui i cyborg possono aiutarci a trascendere la rigidità dell'incarnazione fisica del mondo reale. I discorsi d'odio di genere su Internet sono un esempio utile per sottolineare la centralità della figura del corpo femminile nelle TFSV, nonché le complessità associate all'inquadramento di questi danni. I discorsi d'odio su Internet sono più che episodi isolati o casuali di cyberbullismo. Le folle anonime prendono di mira sistematicamente e in modo sproporzionato le donne come oggetto del loro odio, in particolare le lesbiche o le donne di colore. I danni dell'abuso online, in superficie, possono sembrare disincarnati, ma in realtà gli effetti possono essere sia psichici che fisici[99].

[97] E. Grosz, *Volatile Bodies: Toward a Corporeal Feminism*, cit.

[98] M.C. Nussbaum, *Anger and forgiveness: Resentment, generosity, justice*, Oxford, Oxford University Press, 2016; trad. it., *Rabbia e perdono: la generosità come giustizia*, Bologna, Il mulino, 2017.

[99] D. K. Citron, *Hate crimes in cyberspace*, Cambridge (MA), Harvard University Press, 2014.

Le sfide poste dall'anonimato degli utenti e dai confini giurisdizionali rendono l'individuazione e la punizione sempre più sfuggenti. I quadri giuridici sono semplicemente inadeguati ad affrontare i tipi di danni perpetrati da questi comportamenti. In altre parole, la questione del danno – virtuale, incarnato o entrambi – non è adeguatamente colta dalle tradizionali risposte della giustizia penale e civile. È fondamentale considerare i danni delle TFSV sia in termini collettivistici che individualistici. Ad esempio, la mentalità di gruppo di questi vari comportamenti può consolidare e radicalizzare opinioni sessiste, razziste e omofobe, e persino incitare alla violenza fisica nel cosiddetto mondo offline. Le dinamiche di gruppo sono anche in grado di diffondere la responsabilità morale o giuridica dei membri del gruppo, spostare la responsabilità, fornire un maggiore anonimato e disumanizzare e colpevolizzare le vittime in modi mai immaginati prima.

L'assenza di contatto visivo e la non identificabilità (cioè la non divulgazione di informazioni personali potenzialmente identificabili) in molte interazioni online giocano un ruolo importante nel facilitare i comportamenti aggressivi online[100]. Il danno psicologico è anche un danno fisico e sociale, incarnato e reale. Questa concezione del danno come vissuto e sociale può aiutare a collocare la centralità del corpo nella perpetrazione degli abusi online, nonostante le affermazioni contrarie che affermano l'assenza o la sospensione del corpo fisico nel cyberspazio.

Il concetto di stupro virtuale fornisce un esempio utile e paradigmatico per riflettere sul problematico dualismo mente/corpo e sugli effetti che la vittimizzazione sessuale online può avere[101]. Lo stupro virtuale può essere equiparato moralmente allo stupro fisico. La gravità di uno stupro virtuale è paragonabile a quella di uno stupro fisico, ma si osserva che il primo si verifica più frequentemente del secondo a causa di un'asimmetria tra la gravità dell'atto e la sua percezione comune[102]. Questa asimmetria potrebbe derivare dall'anonimato come stimolo alla violenza, nonostante altri elementi tecno-sociali e spazio-sociali come l'invisibilità, l'asincronicità, l'introiezione solipsistica, l'immaginazione dissociativa e la minimizzazione dell'autorità rafforzino tale ipotesi.

Fraser ha evidenziato che nel contesto del mondo digitale globalizzato, le ingiustizie non sono più confinate entro i confini nazionali. Questo è particolarmente evidente nello spazio online, dove i protagonisti e la tecnologia possono trovarsi in luoghi diversi, creando una mancanza di regolamentazione legale efficace. Ciò influisce direttamente sulla possibilità di ottenere giustizia: chi può chiedere un risarcimento? A chi rivolgersi per ottenere giustizia? Come gestire le leggi e i rimedi in un contesto globale?[103]

È rilevante sottolineare che il terzo aspetto della giustizia secondo Fraser riguarda la rappresentanza politica, ovvero il riconoscimento come cittadini o soggetti di giustizia per poter

[100] M.C. Nussbaum, S. Levmore (Eds.), *The Offensive Internet: Speech, Privacy, and Reputation*, Cambridge (MA), Harvard University Press, 2011.

[101] R. MacKinnon, *Virtual rape*, in "Journal of Computer-Mediated Communication", 2(4), 1997, pp. 1-2.

[102] F. Striano, *The dangerous liaison between rape culture and information technologies: reality, virtuality, and responsibility in cyber-rapes*, in F. Striano, F., M.L. Edwards, S.O. Palermos (Eds.), *Feminist philosophy and emerging technologies*, New York, Routledge, 2023, pp. 74 ss.

[103] N. Fraser, *Scales of Justice: Reimagining Political Space in a Globalizing World*, New York, Columbia University Press, 2009.

avanzare e far valere le proprie rivendicazioni. Questo solleva il dilemma su come i nostri sé globali e digitali possano essere considerati cittadini o soggetti di giustizia.

Fraser suggerisce l'importanza di un movimento femminista globale o transnazionale. Questo movimento dovrebbe riformulare l'ineguaglianza di genere come un problema che coinvolge molteplici siti – sia locali che globali – e che sono interconnessi e reciprocamente rafforzati. Un inquadramento femminista globale delle TFSV deve quindi considerare la natura di genere, la tecno-socialità e la disuguaglianza di status o il misconoscimento che costituiscono questi danni, evitando di cadere nella trappola dell'universalizzazione.

8. Aspetti teorici del cyberstalking

La significativa diffusione di piattaforme social come Facebook, Instagram, TikTok e Metaverso ha condotto alla commercializzazione delle relazioni sociali e delle informazioni personali[104]. Di conseguenza, le persone sono spinte a pubblicare online profili personali, interessi, blog, foto, video e diari, spesso condividendo pensieri e desideri che altrimenti rimarrebbero segreti[105]. Queste informazioni personali offrono uno sguardo sulle fantasie, sulle insicurezze e sugli alter ego delle persone. Questa ampia divulgazione di informazioni personali probabilmente agevola e quindi promuove il cyberstalking[106]. L'abilità di cyber-stalkare è cresciuta anche grazie agli strumenti di social networking geolocalizzanti come "SocialRadar" e all'utilizzo di sistemi intelligenti che consentono un *data mining* più sofisticato[107]. Questi sistemi incoraggiano attivamente gli utenti a condividere informazioni personali, mentre strumenti sofisticati ne permettono la raccolta e l'analisi su vasta scala. Eppure, le sole opportunità e facilitazioni non sono sufficienti per spiegare completamente il comportamento deviante. Attualmente, le politiche esistenti mirate a prevenire i crimini informatici risultano inefficaci e lasciano le vittime indifese[108].

Un approccio eminentemente legalistico che propone una regolamentazione del cyberstalking spesso trascura l'analisi del cyberspazio da una prospettiva sociale più ampia, concentrandosi esclusivamente sulla concezione del cyberspazio come mero prolungamento del mondo reale[109]. Questa focalizzazione eccessiva sull'aspetto normativo convenzionale potrebbe sovrastimare l'efficacia della legislazione esistente, trascurando così altre modalità più efficaci di regolamentazione. La società digitale rappresenta una vera rivoluzione sociale che richiede una

[104] R. Longhurst, *Skype: Bodies, screens, space*, London, Taylor & Francis, 2016.

[105] A.M. Lomanowska, M.J. Guitton, *Online intimacy and well-being in the digital age*, in "Internet interventions", 4, 2016, pp. 138 ss.

[106] B.H. Spitzberg, W. R. Cupach, *The dark side of relationship pursuit: From attraction to obsession and stalking*, London, Routledge, 2014.

[107] K. J. Mitchell *et al.*, *Use of social networking sites in online sex crimes against minors: An examination of national incidence and means of utilization*, in "Journal of Adolescent Health", 47(2), 2010, pp. 183 ss.

[108] S. Basu, *Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis*, in "European Journal of Law and Technology", 3(2), 2012, pp. 1 ss.

[109] R. Moore, *Cybercrime: Investigating high-technology computer crime*, London, Routledge, 2014.

nuova comprensione sociologica e, di conseguenza, nuove basi normative che tengano conto sia della natura delle attività coinvolte sia dello spazio virtuale in cui si svolgono.

In merito alla definizione di cyberstalking, emerge un'assenza di coerenza sia nella legislazione che nella ricerca accademica[110]. Questo concetto risulta ancora controverso e necessita di un'analisi approfondita all'interno di un quadro teorico adeguato. Una definizione operativa proposta identifica il cyberstalking come un insieme di comportamenti minacciosi o avances indesiderate perpetrati attraverso mezzi tecnologici di comunicazione elettronica.

Nel dibattito accademico sul cyberstalking, si evidenziano due principali posizioni: una che lo considera semplicemente come un'estensione dello stalking tradizionale offline[111], in cui Internet funge da strumento aggiuntivo per gli stalker; e un'altra che lo interpreta come una forma criminale distinta non direttamente correlata allo stalking tradizionale[112]. Mentre alcuni studiosi sottolineano le somiglianze tra lo stalking online e offline, come il desiderio di controllo sull'avversario[113], altri enfatizzano le differenze sottolineando la natura unica del cyberstalking rispetto al suo equivalente fisico[114].

A mio avviso, il cyberstalking non è semplicemente definibile come lo stalking tramite Internet. Ci sono differenze qualitative tra lo stalking nello spazio fisico e lo stalking nel cyberspazio[115]. La crescente attenzione giuridica alla criminalità informatica ha reso necessaria anche la necessità di stabilire le differenze tra i crimini nel mondo fisico e i crimini nel mondo digitale[116]. Ad avviso di alcuni studiosi[117], esistono tre tipi di crimini informatici: i crimini tradizionali in cui Internet è uno strumento di supporto, i crimini ibridi che sfruttano nuove opportunità offerte da Internet e i veri crimini informatici esclusivamente prodotti dal cyberspazio.

Il cyberstalking, a prima vista, sembra essere un crimine ibrido che espande possibilità devianti già esistenti. Ma, a mio avviso, le differenze significative tra lo stalking offline e online rendono improprio descrivere il cyberstalking come una mera variante dello stalking fisico. La legge deve affrontare le questioni giuridiche legate alla realtà virtuale, come lo stalking di un individuo virtuale, poiché il sistema giuridico attuale non è preparato per affrontare i crimini virtuali commessi da identità virtuali[118].

[110] C. Hine, *Ethnography for the internet: Embedded, embodied and everyday*, London, Routledge, 2020.

[111] J.A. Davis (Ed.), *Stalking crimes and victim protection: Prevention, intervention, threat assessment, and case management*, Boca Raton, CRC Press, 2001.

[112] A. Adam, *Gender, ethics and information technology*, Berlin, Springer, 2005.

[113] C. Greer, News media criminology, in E. McLaughlin, T. Newburn (Eds.), *The SAGE handbook of criminological theory*, 2010, pp. 490-513.

[114] G. Lastowka, *Virtual justice*, New Haven, Yale University Press, 2010.

[115] S. Chng *et al.*, *Hacker types, motivations and strategies: A comprehensive framework*, in "Computers in Human Behavior Reports", 5, 2022, pp. 100 ss.

[116] D. Wall, *Cybercrimes: The Transformation of Crime in the Information Age,* Cambridge (UK), Polity Press, 2007.

[117] A. Pattavina (Ed.), *Information Technology and the Criminal Justice System,* Thousand Oaks (CA), Sage, 2005.

[118] T. Holt, A. Bossler, *Cybercrime in progress: Theory and prevention of technology-enabled offenses*, London, Routledge, 2015.

Le differenze tra stalking e cyberstalking sono rilevanti; pertanto, i principi giuridici relativi allo stalking non dovrebbero essere applicati sic et simpliciter al cyberstalking. Nel cyberspazio, la mancanza di stimoli senso-percettivi può favorire fraintendimenti sulle intenzioni, promuovendo un falso senso di intimità. La facilità d'uso e l'anonimato delle comunicazioni online possono incentivare il cyberstalking, creando una nuova dinamica dannosa in cui gli stalker possono agire a distanza senza esitazione. La fusione tra devianza e controlli si traduce in una nuova geometria del danno, in cui un potenziale stalker che potrebbe non essere disposto o non essere in grado di affrontare una vittima di persona o al telefono può mostrare poca esitazione a dispensare danni a distanza inviando comunicazioni elettroniche moleste o minacciose a una vittima.

Queste differenze sottolineano la necessità di trattare il cyberstalking in modo distinto dallo stalking fisico, poiché le caratteristiche uniche del cyberspazio richiedono approcci giuridici specifici per affrontare questa forma di crimine[119].

Questa mancanza di consapevolezza fa sì che il danno subito dalle vittime del cyberstalking venga spesso ignorato. Nella comunicazione faccia a faccia, gli individui sono vincolati dalle regole sociali che governano l'interazione interpersonale, dal feedback negativo immediato e dalle conseguenze visibili del loro comportamento inappropriato[120]. Nel cyberspazio, invece, è noto che le persone adottano comportamenti anti-normativi. La perdita delle restrizioni può portare le persone a comportarsi in modo meno altruistico; si sentono meno inibite e si esprimono più apertamente[121]. La tentazione di impegnarsi in comportamenti sconsiderati, impulsivi e disinibiti aumenta la probabilità di cyberstalking. Inoltre, fornisce al cyber-stalker l'opportunità di arruolare la partecipazione di terzi, i cui conseguenti comportamenti aggravano l'intensità della sofferenza della vittima. Una vittima di solito ha solo le parole dell'autore del reato da interpretare online.

La seconda differenza riguarda la relazione tra stalker e vittima. Nel mondo fisico, le informazioni raccolte da un individuo sono limitate alle personalità pubbliche, alle relazioni passate e ai vicini. Ma, su Internet, la vicinanza elettronica permette il cyberstalking da parte di estranei[122]. Le vittime online spesso non comprendono l'intimità istantanea offerta da Internet, facilitando la condivisione di informazioni personali con sconosciuti. Questa falsa sensazione di intimità può essere seducente, portando a una differenza qualitativa tra stalking offline e online.

La terza differenza riguarda la natura degli atti. I cyberstalker si concentrano su attività diverse dallo stalking fisico, sfruttando il cyberspazio per monitorare le vittime a vari livelli, partecipando a forum, cercando informazioni online e persino accedendo al computer della vittima. Benché monitorare una vittima online aumenti il rischio di essere scoperti, tale pratica fornisce al cyberstalker maggiori informazioni e contatti con la vittima, alimentando fantasie voyeuristiche e il desiderio di controllo. Il monitoraggio online è meno rischioso rispetto a quello fisico,

[119] R. Brownsword, *Law, technology and society: reimagining the regulatory environment*, London, Routledge, 2019.

[120] M. McGuire, *Hypercrime: The New Geometry of Harm,* London, Routledge-Cavendish, 2007.

[121] D. Wall (Ed.), *Crime and the Internet*, London, Routledge, 2003.

[122] S. Basu, R. Jones, *Regulating Cyberstalking*, in F. Schmalleger, M. Pittaro (Eds.), *Crimes of the Internet,* Upper Saddle River, Prentice Hall, 2008, pp. 141 ss.

poiché poche vittime possono rilevare tecnologicamente un tale comportamento[123]. Queste differenze rendono il cyberstalking concettualmente e empiricamente distinto dallo stalking tradizionale.

I casi di cyberstalking sono probabilmente più numerosi di quanto sostenuto dalle forze dell'ordine, dai media o dai critici, e gli episodi di cyberstalking sono aumentati notevolmente negli ultimi anni. Sebbene non esistano studi che documentino accuratamente la portata del cyberstalking, questo fatto può essere illustrato dal numero crescente di segnalazioni relative alle molestie online. Il cyberstalking non può essere affrontato semplicemente modificando i principi che utilizziamo per imporre la responsabilità per lo stalking nel mondo fisico; dobbiamo creare un nuovo reato, che comprenda l'*actus reus* e la *mens rea*[124].

Le protezioni giuridiche contro il cyberstalking per essere realmente efficaci devono affrontare le questioni sociali e politiche, insieme alle sfide nell'individuazione, identificazione, raccolta di prove, attribuzione e giurisdizione. Sebbene gli aspetti del cyberspazio possano sembrare immaginari, le conseguenze che i partecipanti che abitano questi spazi devono affrontare sono molto reali. In questo contesto, quali sarebbero i ruoli delle tradizionali difese e sanzioni? A chi spettano gli obblighi di regolamentazione e responsabilità? Le risposte politiche a questa situazione spesso si limitano a ripristinare la trasparenza di comportamenti potenzialmente criminali senza comprendere la vera natura del reato e chi ne è afflitto. C'è una relazione simbiotica tra un individuo e un'identità sociale, basata sulla categorizzazione per determinare l'accettabilità dell'appartenenza a determinati gruppi sociali. La persona e l'identità della vittima acquisiscono quell'identità sociale mediante l'associazione con una comunità nel cyberspazio. Inoltre, è l'anonimato di Internet che solleva la questione di cosa costituisca comportamenti normali e devianti.[125]

In una società dominata da norme sociali che tutelano l'identità sociale, ogni comportamento che violi la norma è considerato deviante e quindi soggetto a sanzioni. La chiave è consentire la identificazione dei membri anonimi quando sono implicati in attività dannose. Questo richiederebbe un cambiamento significativo nei metodi di applicazione della legge per quanto riguarda la sorveglianza e le indagini.

Un problema rilevante per la regolamentazione del cyberstalking riguarda la distinzione tra quali comportamenti dovrebbero essere sanzionati e chi dovrebbe essere responsabile delle indagini e dell'applicazione delle sanzioni. Date le caratteristiche del cyberspazio, concentrarsi sull'applicazione delle norme risulterebbe essere inefficace. Alcuni studiosi ritengono che le leggi verranno rispettate solo se sono considerate valide, ossia se le disposizioni sono ben definite, giustificabili e derivano da un'autorità legittima. Ma quanto possono essere efficaci le leggi adattate da quelle progettate principalmente per affrontare le molestie e lo stalking fisico?

Le leggi contro le molestie offrono alcuni rimedi, ma sono complesse a causa della varietà di norme che possono essere impiegate per perseguire un colpevole. Anche se potrebbe essere

[123] Y. Jewkes (Ed.), *Dot. Cons: Crime, Deviance and Identity on the Internet,* Collumpton, Willian, 2002.

[124] S.W. Brenner, *Is there such a thing as 'Virtual Crime'?*, in "California Criminal Law Review" 4(1), 2001, pp. 1-72.

[125] E. Martellozzo, E.A. Jane (Eds.), *Cybercrime and its victims,* London, Taylor & Francis, 2017.

fattibile applicare le leggi attuali quando il danno è subito da una persona offline, sarebbe problematico estendere tali leggi a nuove vittime il cui coinvolgimento nel reato avviene esclusivamente online. Inoltre, si ignora il fatto che il cyberstalking comprende un'ampia gamma di nuovi comportamenti non associati allo stalking offline[126].

Esaminando le differenze tra stalking fisico e cyberstalking, il carattere del cyberspazio e i suoi effetti sulle interazioni sociali, la natura dei legami sociali e la portata dell'esperienza e della realtà, alcuni studiosi si opposero alla regolamentazione perché, una volta implementata, avrebbe non solo regolamentato i comportamenti devianti, ma avrebbe anche criminalizzato alcune forme di comportamento legittimo[127].

9. Comunitarismo digitale

La natura della regolamentazione dipende dalla categorizzazione di un crimine. Occorre fare una chiara distinzione tra crimine informatico puro e crimine informatico ibrido. Il puro crimine informatico richiede una combinazione di azione legale privata e tecnologia, o un approccio realista digitale[128].

Questo ci porterebbe a sottocategorizzare il cyberstalking per distinguere tra (1) una mera estensione dello stalking fisico, in cui la vittima è conosciuta dallo stalker e la tecnologia è semplicemente utilizzata per offrire nuove opportunità e (2) il puro cyberstalking, in cui la vittima e lo stalker possono essere nascosti in pseudo personaggi all'interno di un mondo virtuale lontano e rimosso dalla realtà.

Probabilmente è più utile sviluppare un processo attraverso il quale il cyberstalking dovrebbe essere affrontato in futuro. La natura dell'attività e la comunità virtuale in cui si svolge richiedono una revisione più radicale delle questioni implicate. Non possiamo limitarci a ricorrere alle soluzioni legislative o tecnologiche esistenti. La questione si riduce alla necessità percepita di regolamentare questo particolare comportamento: il cyberstalking nel cyberspazio[129].

I legislatori e gli scrittori immersi nello stato di diritto vedono l'unica soluzione in una qualche forma di regolamentazione basata su standard giuridici. Fissata nel mondo fisico, la regolamentazione imposta, formale e burocratica è un dato di fatto, imposto dall'alto e vincolato a regole. Diversamente da questo modello formale, è preferibile percorrere una strada regolativa alternativa, bottom-up, basata sul concetto di comunità virtuale. Le comunità e le attività prosperano nella Rete senza meccanismi di regolazione formale.

[126] L. Ellison, Y. Akdeniz, *Cyberstalking: The regulation of harassment on the internet*, in D. Wall (Ed.) *Cyberspace Crime*. London, Routledge, 2017, pp. 275 ss.

[127] N. Tsagourias, *The legal status of cyberspace*, in *Research handbook on international law and cyberspace*. Cheltenham, Edward Elgar Publishing, 2015, pp. 13 ss.

[128] D. Wall, *Digital realism and the governance of spam as cybercrime*, in "European journal on criminal policy and research", 10, 2004, pp. 309 ss.

[129] S.W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, in "California Criminal Law Review", 4(1), 2001, p. 53.

Pertanto, è necessario concentrarsi sullo sviluppo di un modello per comprendere come il cyberspazio possa essere controllato socialmente, considerando gli aspetti di formalità/informalità, visibilità/invisibilità e la natura e l'entità delle reazioni ai comportamenti devianti.[130]

I sistemi giuridici non sempre offrono soluzioni coerenti e prevedibili per i problemi sociali percepiti. Il cyberspazio ha esteso i confini della regolamentazione legale oltre la sua capacità e quindi i regolatori hanno cercato di applicare una forma di regolamentazione formale e universale alle comunità virtuali e ai loro partecipanti spesso anonimi, il che sembra poco praticabile. Le leggi non stabiliscono automaticamente le norme. La maggior parte delle comunità virtuali ha già stabilito delle regole per regolare il comportamento. L'introduzione di nuove leggi per regolare le comunità virtuali, che entrano in conflitto con le norme esistenti, potrebbe portare al loro disinteresse.

La stragrande maggioranza degli utenti nel cyberspazio agisce legalmente. Come possiamo garantire che continuino a farlo? Lessig ha affermato che il cyberspazio presenta qualcosa di nuovo per quelli di noi che pensano alla regolamentazione e alla libertà. Richiede una nuova comprensione di come funziona la regolamentazione e di cosa regola la vita lì[131].

Quindi, l'interrogativo fondamentale è come creare una regolamentazione efficace che mantenga il controllo solo sul comportamento deviante dell'individuo all'interno delle comunità virtuali.

Per risolvere il problema della corretta applicazione del diritto nello spazio cibernetico, dovremmo concentrarci sulla progettazione di un sistema di regolamentazione che garantisca flessibilità, responsabilità e tempestività nella decisione. È necessario disporre di un insieme di regole più flessibili e adatte a contesti più specifici. Queste regole, individuate nei codici di condotta, costituiscono linee guida di buone pratiche sviluppate attraverso l'esperienza e il controllo, rappresentano un sistema volontario di regolamentazione basato sul reciproco riconoscimento delle norme stabilite all'interno di una comunità virtuale. Questi codici vengono formulati e concordati come standard di condotta etica che gli individui all'interno di una comunità virtuale dovrebbero seguire in modo razionale piuttosto che arbitrario. Basati sul principio che il diritto penale punisce i reati contro la "coscienza collettiva", tali codici di condotta prescrivono modalità di comportamento che enfatizzano o normalizzano particolari forme di relazione e potrebbero essere utilizzati per sviluppare parametri di riferimento e migliori pratiche che promuovano strategie normative e di applicazione future. Le comunità virtuali trarrebbero vantaggio nello sviluppare disposizioni che definiscano chiaramente ciò che è o non è consentito all'interno della comunità.

Una caratteristica distintiva chiave dei codici di condotta è che si originano da una decisione individuale di comportarsi in modi particolari all'interno della comunità virtuale. Tale comportamento crea aspettative per gli altri osservatori, che si sentono obbligati a emularlo[132]. In altre parole, i codici di condotta si svilupperebbero spontaneamente dal basso verso l'alto, anziché

[130] R. Brownsword, *In the year 2061: from law to technological management*, in "Law, Innovation and Technology", 7(1), 2015, pp. 1 ss.

[131] L. Lessig, *Code and other Laws of Cyberspace,* New York, Basic Books, 1999.

[132] R.M. Kramer (Ed.), *Organizational trust: A reader*. Oxford management readers, 2006.

essere imposti intenzionalmente attraverso la legislazione. Inoltre, sarebbero accettati volontariamente dai partecipanti alla comunità virtuale.

Un aspetto rilevante di questo metodo di regolamentazione riguarda il concetto di "contesti condivisi". In queste situazioni, le persone interagiscono su un terreno comune e le relazioni tra i partecipanti non dipendono esclusivamente dalla sostenibilità a lungo termine o dall'interazione diretta e personale. In altre parole, il contesto e il contenuto (o attività) sono strettamente connessi.

Un sistema del genere sarebbe particolarmente efficace nel regolare il cyberstalking e tutti quei comportamenti sociopatici associati alle piattaforme dei social network. La distinzione tra le norme stabilite dalla comunità online e quelle imposte dai governi risiede nel fatto che le prime sono vincolanti solo per i membri di una specifica comunità virtuale autoimposta, mentre le seconde hanno un'applicabilità più ampia e universale.

In linea di principio, questo sistema potrebbe funzionare poiché controllerebbe esclusivamente i comportamenti devianti nel cyberspazio, persuadendo gli attori umani a adottare comportamenti desiderabili attraverso una valutazione adeguata del contesto. In una situazione ideale, tali codici di condotta verrebbero diffusi all'interno delle comunità virtuali mediante la condivisione. Se una comunità virtuale è riconosciuta per la capacità di fornire una protezione efficace, altre comunità virtuali dovrebbero essere in grado di utilizzare tali codici di condotta come punto di riferimento.

Pertanto, l'implementazione di codici di condotta come norme giuridiche potrebbe essere necessaria per integrare la regolamentazione e proteggere efficacemente le parti più vulnerabili. In altre parole, dando considerazione al fatto che il cyberspazio presenta una natura individualistica, è difficile da disciplinare in base alle tradizionali categorie giuridiche, mentre i codici di condotta basati sul rispetto reciproco, che seguono i valori del consenso dei soggetti governati e che sono progettati per affrontare l'autonomia di una comunità virtuale, potrebbero dimostrarsi efficaci[133]. Una volta sviluppati e implementati, i codici di condotta contribuiranno a ridurre l'indifferenza e a favorire un'incrementata conoscenza reciproca.

Un ulteriore problema legato all'applicazione della legge è la questione della legittimità delle leggi in un contesto inter-giurisdizionale. I codici di condotta possono contribuire attivamente a prevenire crisi di legittimità in quanto non sono vincolati ad alcuna giurisdizione particolare.

Un esempio in questo contesto potrebbe riguardare la "cyber-socializzazione" all'interno delle comunità virtuali e le eventuali conseguenze, come il cyberstalking. La mia posizione è che, all'interno delle comunità virtuali, la regolamentazione del comportamento deviante si è sviluppata rapidamente negli ultimi anni, principalmente evolvendo da un movimento di vigilanti a un modello di polizia formale.

Man mano che gli individui all'interno di una comunità virtuale si impegnano in modo cooperativo, stabilendo relazioni bilaterali di successo e rispettando i codici di condotta stabiliti, è probabile che altri ne notino il comportamento cooperativo e cerchino di avviare relazioni reci-

[133] D.G. Post, *Governing cyberspace*, in P.S. Berman (Ed.) *The Globalization of International Law*, London, Routledge, 2017, pp. 57 ss.

procamente vantaggiose con loro. Una volta raggiunto un livello generale di conformità, è probabile che si crei un obbligo che garantisca che tutti i membri rispettino tali regole, per il bene comune della comunità.

La risposta della comunità virtuale di fronte a un individuo che violi i codici di condotta sarebbe fondamentale per preservare l'integrità della comunità come istituzione sociale. Qualsiasi comportamento deviante che minacci tali codici verrebbe considerato un'offesa ai "sentimenti collettivi", e ciò potrebbe giustificare l'applicazione di sanzioni da parte della comunità virtuale.

La decisione di imporre sanzioni dovrebbe essere presa esclusivamente dalla comunità stessa, agendo come un arbitro tramite il "consenso positivo". È importante sottolineare che la divulgazione di informazioni sul comportamento deviante di un individuo potrebbe legittimamente mettere a rischio tutte le relazioni benefiche che l'individuo ha stabilito all'interno della comunità virtuale.

I codici di condotta consentiranno ai membri della comunità di andare ben oltre la semplice definizione di una norma; sarebbero in grado di realizzare interventi di governo della comunità virtuale. Ciò comporterebbe il rispetto incondizionato dei codici di condotta da parte di chiunque scelga di entrare in qualsiasi forma di interazione, insieme al rifiuto di interagire con qualsiasi individuo noto per aver adottato un comportamento indesiderabile all'interno della comunità.

Questa pressione collettiva a conformarsi ai codici di condotta potrebbe notevolmente aumentarne l'efficacia come deterrente. La non conformità, infatti, potrebbe esporre l'individuo a un rischio maggiore di isolamento dalla comunità, poiché la reputazione del membro all'interno della comunità funge da vincolo che andrebbe perduto in caso di mancata dimostrazione di affidabilità.

Il confronto tra libertà sociali e sicurezza individuale è spesso evidenziato nei dibattiti sulle comunità virtuali. Questo si è manifestato, ad esempio, nel caso del cyberstalking, in cui lo status illegale del comportamento inaccettabile può dipendere da leggi che non affrontano direttamente la criminalità percepita.

È fondamentale diffondere tali codici di condotta tra tutti i membri di una comunità virtuale e incentivare fortemente il loro utilizzo al fine di garantire l'efficacia del sistema di controllo. Sebbene questa analisi sia generalmente corretta per quanto riguarda la domanda a cui tenta di rispondere, è importante comprendere che l'efficacia dei codici di condotta sarà limitata al cyberstalking che avviene all'interno di una comunità virtuale, poiché sono progettati per mantenere l'ordine interno di tale comunità. È importante riconoscere che potrebbero esserci problemi di imprevedibilità per quanto riguarda l'accettazione tra i primi utilizzatori, dato che potrebbe esserci un divario tra ciò che dovrebbero far rispettare i codici di condotta e come vengono realmente applicati nella pratica.

Inoltre, i vincoli pratici possono limitare l'applicazione delle sanzioni nel cyberspazio, poiché gli utenti possono assumere più identità. Per superare questo problema, potrebbe esserci la necessità di limitare agli utenti la creazione di più di un account, anche se ciò potrebbe compor-

tare una minore adesione alla comunità o il rischio che gli utenti aggirino il problema registrandosi con diversi indirizzi email[134]. Questo complicherebbe ulteriormente l'analisi dell'applicazione delle sanzioni. Tuttavia, ritengo che implementando un meccanismo di analisi della reputazione, simile a quello adottato da eBay, insieme alle sanzioni, sia possibile ridurre il numero di comportamenti devianti e il numero di identità virtuali create da un singolo utente[135].

È del tutto plausibile che le carenze sanzionatorie dei codici di condotta possano essere sfruttate da una comunità troppo entusiasta e troppo vigile. Ad esempio, l'isteria comunitaria associata a false denunce di abuso può portare a discriminazione contro gli individui presi di mira, mediante l'impiego di minacce coercitive e all'eventuale imposizione di altre regole che vanno oltre le norme che i membri della comunità dovrebbero seguire[136].

L'ulteriore eterogeneità di interessi potrebbe generare problemi nell'applicazione dei codici di condotta. Dato che gli individui sono esposti a influenze e circostanze diverse, è inevitabile che non tutti i membri di una comunità virtuale siano ugualmente coinvolti nei "sentimenti collettivi".

All'aumentare delle dimensioni di una comunità, diminuisce la probabilità che tutti i suoi membri condividano interessi comuni. Di conseguenza, i membri potrebbero cominciare a sentirsi anonimi e quindi meno legati socialmente nelle loro azioni. Inoltre, potrebbero sorgere interessi contrastanti e problematiche di fiducia tra i membri della comunità.

Questa situazione è particolarmente probabile quando gli incentivi vengono distribuiti in modo asimmetrico all'interno della comunità. In una simile circostanza, i codici di condotta possono essere utilizzati per gestire il conflitto, bilanciando attentamente gli interessi dell'individuo con quelli della comunità. Anche se ciò non sempre eliminerà il conflitto. I codici di condotta potrebbero risultare in un potere contrattuale superiore per la parte prevalente, causare problemi di azione collettiva per i dissidenti o comportare l'utilizzo di strategie da entrambe le parti.

Inoltre, un'obiezione frequente a un sistema di regolamentazione volontario è il problema percepito dell'applicabilità in assenza di persuasione esterna. Si riconosce che l'effettiva attuazione dei codici di condotta dipenderebbe interamente dalle sanzioni sociali, la cui legittimità scaturisce dall'approvazione dei membri della comunità virtuale[137]. Questo implica che i codici di condotta vengono applicati solo nella misura in cui i membri della comunità scelgono di rispettarli[138].

Un'obiezione comune nei confronti dei sistemi di regolamentazione volontaria è che potrebbero rivelarsi inefficaci nel contrastare il comportamento deviante. Secondo questa obiezione, solo i membri che già rispettano le regole le seguiranno, mentre gli altri continueranno a violarle impunemente. Tuttavia, questa obiezione ignora l'importanza della pressione sociale. La minaccia di ostracismo, disapprovazione o altre sanzioni da parte degli altri membri della comunità può rappresentare un deterrente efficace contro il comportamento deviante.

[134] A. Murray, *The regulation of cyberspace: control in the online environment*, London, Routledge, 2007.

[135] E. Posner, *Law and social norms*, Cambridge (MA), Harvard University Press, 2002.

[136] G.F. Lastowka, D. Hunter, *The laws of the virtual worlds*, in *Popular Culture and Law*, London, Routledge, 2017, pp. 363 ss.

[137] E.J. Stieglitz, *Anonymity on the Internet: How does it work, who needs it, and what are its policy implications*, in "Cardozo Arts & Ent. LJ", 24, 2006, pp. 1395 ss.

[138] W.R. Scott, *Group theory*, North Chelmsford (MA), Courier Corporation, 2012.

Nelle comunità virtuali, dove le relazioni e la reputazione svolgono un ruolo cruciale, la pressione sociale può diventare particolarmente intensa. I membri che violano le regole rischiano di essere isolati, esclusi dai gruppi o addirittura soggetti a pubbliche denunce. Pertanto, la minaccia di sanzioni sociali può costituire uno strumento importante per far rispettare i codici di condotta all'interno delle comunità virtuali. Questa strategia, unita all'educazione e alla sensibilizzazione, può contribuire a creare un ambiente online più sicuro e piacevole per tutti gli utenti.

In definitiva, l'efficacia di un sistema di regolamentazione volontaria dipende da diversi fattori, quali la natura della comunità, la gravità del comportamento deviante e l'esistenza di adeguate sanzioni sociali. La pressione sociale può rappresentare un potente strumento per promuovere il rispetto delle regole e la coesione sociale nelle comunità virtuali. Un potenziale problema potrebbe derivare dal fatto che solamente i membri della comunità virtuale che osservano i codici di condotta non sarebbero in primo luogo responsabili del comportamento deviante. Tuttavia, tale obiezione non tiene conto dell'efficacia della minaccia di sanzioni da parte degli altri membri del gruppo, che contribuirebbero notevolmente al normale funzionamento delle comunità virtuali.

9. Conclusione

Il cyberspazio è subordinato allo spazio fisico o separato da esso? Esiste una relazione circolare e produttiva tra il cyberspazio e lo spazio fisico? Secondo McGuire, il cyberspazio non è distinto dallo spazio fisico; al contrario, mantiene al suo interno tutte le forme limitate di interazione spaziale, pur estendendole e complessificandole[139]. Questa affermazione può essere dimostrata in vari modi, inclusa la visualizzazione della sua struttura, l'analisi quantitativa e la creazione di una geografia del cyberspazio[140].

Questo non implica fare a meno del concetto di cyberspazio perché fuorviante ma rivalutarne le sue peculiarità: il cyberspazio non è solo la sua onnipresenza o ubiquità, ma è anche il senso di intimità che crea. Questo ambiente cyber-sociale completamente nuovo ha sfruttato in modo creativo le caratteristiche del sistema per giocare con nuove forme di comunicazione espressiva, per esplorare possibili identità pubbliche, per creare relazioni altrimenti improbabili e per stabilire norme comportamentali. In questo modo, il cyberspazio ha inventato nuove comunità virtuali e ha collaborato alla costruzione di un senso dello spazio e del luogo. Sebbene siano state condotte numerose ricerche per esaminare un'ampia varietà di questioni che operano a vari livelli all'interno delle comunità virtuali, poche hanno esplorato congiuntamente il processo di costruzione di identità e relazioni sociali all'interno di tali ambienti.

Tradizionalmente, la geografia e la vicinanza emotiva hanno contribuito a definire la comunità. Sebbene la geografia continui a essere importante per la definizione di una comunità virtuale, nel contesto di Internet risulta più utile adottare una concezione esperienziale piuttosto

[139] S. Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace,* Cambridge (MA), The MIT Press, 2003.

[140] R. Brownsword, *Rights, Regulation, and the Technological Revolution, Oxford,* OUP, 2008.

che geografica della comunità. Le comunità virtuali vengono definite da Rheingold come aggregazioni sociali che emergono dalla Rete quando un numero sufficiente di persone intraprende discussioni su argomenti di interesse pubblico in modo sufficientemente continuo e rispettoso delle regole sociali[141].

Un utente del sistema può determinare il percorso di relazione ottimale, cioè il percorso di contatto, per raggiungere gli individui desiderati. Gli individui all'interno del sistema possono presentarsi e avviare una comunicazione diretta.

Non tutti gli studiosi accettano le sottoculture informatiche come degne di attenzione, descrivendole come comunità effimere e immaginarie. Vengono considerate troppo fugaci, superficiali e virtuali per meritare un'esplorazione seria[142]. Il concetto di comunità virtuale risulti ancora inconsistente a causa della mancanza di un modello architetturale condiviso su ciò che esattamente costituisce una comunità nel cyberspazio[143].

Inoltre, sorgono interrogativi riguardo al modo in cui le relazioni sociali possono essere mantenute all'interno di una comunità virtuale in un contesto tecnologico come questo, dove le interazioni tra i partecipanti avvengono a distanza. La capacità dei media di ampliare la gamma delle nostre esperienze può creare l'illusione di un maggior contatto o di un'appartenenza a organizzazioni sociali su larga scala. Anziché creare vere e proprie comunità, il cyberspazio sembra sviluppare identità categoriali o comunità immaginarie.

L'approccio proposto potrebbe essere più appropriato teorizzando che le comunità online possono soddisfare il desiderio di vicinanza associato alla *gemeinschaft*. Tale legame sociale è stato del tutto abbandonato nella società contemporanea, in cui la disconnessione sociale della *gesellschaft*, o il predominio dell'interesse personale, si è definitivamente affermata.

Ciò solleva la questione di quanto sia inquietante trovare una comunità attraverso lo schermo di un computer. Molti analisti hanno parlato della vicinanza e della fiducia che nascono da queste connessioni mediate, utilizzando termini come "pseudo-gemeinschaft", intimità virtuale o comunità immaginata. Tali definizioni reificano le interazioni che mancano di un contatto faccia a faccia e le considerano in qualche modo inferiori rispetto alla realtà[144].

Nondimeno, la comunicazione non faccia a faccia non è necessariamente priva di presenza. In ambiente virtuale, gli utenti continuano a partecipare alle attività anche quando sono offline.

È innegabile, almeno sin dalla pubblicazione de "La comunità virtuale" di Rheingold, che le amicizie nel cyberspazio, mediate da reti virtuali, possono essere profonde e significative quanto quelle stabilite faccia a faccia[145].

In linea con il lavoro fondamentale di Rheingold, ritengo che il mondo virtuale possa essere considerato indipendente. Considerando il dominio della tecnologia del mondo sintetico, intere

[141] H. Rheingold, *The virtual community, revised edition: Homesteading on the electronic frontier*, Cambridge (MA), The MIT press, 2000.

[142] J. Lockard, *Progressive politics, electronic individualism and the myth of virtual community*, in D. Porter (Ed.), *Internet Culture*, London, Routledge, 2013, pp. 219 ss.

[143] M. Williams, *Policing and cybersociety: the maturation of regulation within an online community,* in "Policing & Society", 17(1), 2007, pp. 59 ss.

[144] S. Bardzell, W. Odom, *The experience of embodied space in virtual worlds: An ethnography of a Second Life community*, in "Space and Culture", 11(3), 2008, pp. 239 ss.

[145] H. Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier*, cit.

società possono essere replicate e operare su piani separati ma complementari[146]. Se adottiamo questi argomenti, le interazioni all'interno del cyberspazio vengono considerate reali dai partecipanti. Tale conclusione comporterebbe che le motivazioni e la natura dei potenziali danni legati alle attività di cyberstalking e alla violenza digitale di genere meritino di essere prese in seria considerazione: i pixel del cyberspazio sono considerati reali dai partecipanti tanto quanto gli atomi del mondo fisico.

10. Bibliografia di riferimento

Amato Mangiameli A.C., Saraceni G., *I* reati informatici*. Elementi di teoria generale e principali figure criminose*, Torino, Giappichelli, 2019.

Anh N., Deepanjali M., McDowell Z. (Eds.), *Communication Technology and Gender Violence*, Berlino, Springer International Publishing, 2023.

Annoni A., Thiene A. (a cura di), *Minori e privacy. La tutela dei dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, Napoli, Jovene, 2019.

Boyle K., Berridge S. (Eds.), *The Routledge Companion to Gender, Media and Violence*, London, Taylor & Francis, 2023.

Brownsword R., *Rethinking Law, Regulation, and Technology*, London, Edward Elgar Publishing, 2022.

Cockburn C., *Machinery of Dominance: Women, Men and Technical Know-how*, London, Pluto Press, 1985.

Cornelius K., Hermann, D., *Virtual worlds and criminality*, Dordrecht, Springer, 2011.

Criado Perez C., *Invisibili. Come il nostro tempo ignora le donne in ogni campo. Dati alla mano*, Torino, Einaudi, 2020.

Cuklanz L.M., *Gender Violence, Social Media, and Online Environments: When the Virtual Becomes Real*. London, Taylor & Francis, 2022.

Deepanjali M. (Ed.), *Cyberfeminism and Gender Violence in Social Media*, New York, IGI Global, 2023.

Desai M., *Gender and the Politics of Possibilities: Rethinking Globalization*, Washington (DC), Rowman & Littlefield Publishers, 2009.

Edwards M.L., Palermos S.O. (Eds.), *Feminist Philosophy and Emerging Technologies*, London, Routledge, 2023.

Fahri Ö. (Ed.), *Handbook of Research on Digital Violence and Discrimination Studies*, New York, IGI Global, 2022.

Gillespie A., *Cybercrime: Key Issues and Debates*, London, Taylor & Francis, 2015.

Hall M. *et al.*, *Digital Gender-Sexual Violations: Violence, Technologies, Motivations*, London, Taylor & Francis, 2022.

[146] E. Castronova, *Exodus to the virtual world: How online fun is changing reality*, London, MacMillan, 2008.

Hildebrandt M., *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*, London, Edward Elgar Publishing, 2015.

Huberman J., *The Spirit of Digital Capitalism*, London, Polity Press, 2022.

Leimeister J.M., Balaji R., *Virtual Communities*, London, Taylor & Francis, 2015.

Levmore S., Nussbaum M.C. (Eds.), *The Offensive Internet: Speech, privacy, and reputation*, Cambridge (MA), Harvard University Press, 2011.

Maestri E., Thiene A. (a cura di), *Focus on FemTech*, in "BioLaw Journal - Rivista di BioDiritto", 3, 2023, pp. 7-116.

Marion N.E., Twede J., *Cybercrime: An Encyclopedia of Digital Crime*, New York, ABC-CLIO, 2020.

Park Yong J., *The Future of Digital Surveillance: Why Digital Monitoring Will Never Lose Its Appeal in a World of Algorithm-Driven AI*, Ann Arbor, University of Michigan Press, 2021.

Pasquale F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge (MA), Harvard University Press, 2015.

Penny L., *Cybersexism: Sex, Gender and Power on the Internet*, London, Bloomsbury Publishing, 2013.

Rheingold H., *The Virtual Community: Homesteading on the Electronic Frontier*, New York, MIT Press, 2000.

Turkle S., *Alone Together: Why We Expect More from Technology and Less from Each Other*, New York, Basic Books, 2011.

Wall D., *Cybercrime: The Transformation of Crime in the Information Age*, London, Polity Press, 2007.

Yar M., Steinmetz K.F., *Cybercrime and Society*, London, SAGE Publications, 2019.

Zuboff S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, Public Affairs, 2019; trad. it. *Il capitalismo della sorveglianza. Il futuro della umanità*, Milano, LUISS University Press, 2019.

Data di ricezione dell'articolo: 14 marzo 2024
Date di ricezione degli esiti del referaggio in doppio cieco: 20 e 25 marzo 2024
Data di accettazione definitiva dell'articolo: 15 aprile 2024