Università degli Studi di Padova

Dipartimento di Diritto Privato e Critica del Diritto

Corso di Laurea in

Consulente del Lavoro

a.a. 2022-2023

LA CRIMINALITÀ NEL CYBERSPAZIO. CONSIDERAZIONI ETICO-GIURIDICHE E RIFLESSIONI CRITICHE INTORNO AL PRINCIPIO DI TERRITORIALITÀ.

Relatrice: Prof.ssa Mingardo Letizia

Laureanda: Finessi Martina

Matricola: 2003760

RINGRAZIAMENTI

È doveroso per me dedicare un piccolo spazio di questo elaborato al ringraziamento di coloro che con la loro indispensabile presenza nella mia vita, hanno contribuito ad aiutarmi nel raggiungere questo tanto atteso e desiderato traguardo.

In primis, una menzione speciale va a te, nonno Franco: anche se da ormai qualche anno non sei più qui con me, so che mi stai guardando dal cielo e so che mi hai protetta in questi anni e continui a proteggermi, proprio come hai sempre fatto quando ero piccolina e giocavamo insieme al parco o giravamo in bicicletta per le campagne. Grazie per tutto l'affetto che mi hai saputo dare, spero con tutto il cuore di aver reso orgoglioso anche te con questo mio traguardo, ti voglio bene.

Grazie alla nonna Mirella, alla nonna Sandra e al nonno Adriano, punti fermi della mia vita: sono cresciuta assieme a voi e mi avete donato, e continuate a donarmi, quell'affetto speciale che solo i nonni possono dare. Anche se sono tutto tranne che perfetta, so che ai vostri occhi sarò sempre "la più brava del mondo", come dite voi.

Papà Robert e mamma Debora, senza di voi sarei persa, senza di voi non sarei arrivata dove sono ora, il vostro supporto e i vostri incoraggiamenti sono stati fondamentali in questo mio percorso universitario, come lo sono stati anche in tanti altri momenti della mia vita. Grazie perché mi avete dato e continuate a darmi il mondo, grazie perché mi avete sempre spronata a dare il meglio di me, grazie perché avete sempre creduto in me e grazie perché so che su di voi potrò sempre contare, in qualsiasi momento e in qualunque luogo io mi trovi, voi ci sarete sempre per me, come anche io ci sarò sempre per voi.

Grazie anche a tutti gli altri membri della mia famiglia, in particolare allo zio Stefano, alla zia Paola e al mio piccolo cuginetto Liam, che con i suoi sorrisi mi regala sempre tanta gioia e spensieratezza.

Grazie a quella persona che da più di tre anni a questa parte è al mio fianco, nonostante le difficoltà e nonostante la distanza: grazie Mauro, perché sei stato al mio fianco nei traguardi più importanti della mia vita, dal diploma alla laurea, grazie perché abbiamo condiviso tanto e stiamo continuando a condividere tanto insieme, grazie perché sei stato la mia valvola di sfogo nei periodi di studio più stressanti in cui tutto sembrava

essere più grande di me, e grazie perché nei miei momenti di debolezza e sconforto tu sei l'unico che riesce sempre e comunque, con la sua ironia, a strapparmi un sorriso.
Questa laurea la dedico anche a te, a noi, e a quello che ci riserverà il futuro, insieme.
Per la pazienza, per la sopportazione, e per l'aver subito mille lamentele da parte mia, un enorme, immenso e gigantesco Grazie, con la G maiuscola, va alle mie amiche del cuore: Martina Sacchetto, Carlotta e Martina Padovani.
Grazie perché non mi avete mai fatta sentire sbagliata per le mie paranoie, per le mie ansie e insicurezze, grazie perché mi avete saputa capire nei momenti in cui nessun'altro avrebbe potuto farlo meglio di voi, grazie perché è da anni che siete al mio fianco e che condivido con voi tutto, dalle ansie pre-esame, ai concerti, ai viaggi.
Grazie perché senza di voi non saprei come fare, siete fondamentali, vi voglio bene.
Ringrazio anche tutte quelle persone che, anche se non ho esplicitamente menzionato, hanno trascorso del tempo con me durante questi ultimi tre anni, e che anche se non sento ogni giorno, so che sono presenti nella mia vita.
Infine voglio ringraziare me stessa, perché non ho mai mollato, perché non mi sono fermata al primo esame andato male, perché non mi sono mai arresa.
Perché ho fatto fatica, perché ci sono stati dei periodi in cui tutto sembrava andare male e non vedevo la luce infondo al tunnel, periodi in cui avrei solo voluto chiudermi in me stessa e lasciare tutto.
Perché sì, la voglia di mollare tutto c'è stata, non lo nego, ma la mia irrefrenabile voglia di vincere ha sempre prevalso su quella di fallire.
Grazie papà per avermi insegnato che nella vita non bisogna essere deboli e che bisogna reagire alle situazioni e non abbattersi mai, e grazie mamma perché da te ho ereditato la pazienza, che in certe situazioni è indispensabile per riuscire ad andare avanti.
Questa laurea la dedico alla Martina del passato, timida e insicura, alla Martina del presente, ambiziosa e determinata, e a quella del futuro che verrà.
Martina, ci sei riuscita: sei Dottoressa in Consulente del Lavoro.

INDICE

INTRODUZIONE

Con il presente elaborato si vuole evidenziare il tema dell'applicazione del principio di territorialità ai reati informatici, ovvero quegli illeciti che sono compiuti in una sorta di spazio-non-spazio, chiamato *cyberspazio*.

La riflessione parte dalle origini, quindi dall'avvento della Terza e della Quarta rivoluzione industriale, le quali hanno portato ad una crescita del settore informatico fra l'invenzione del Personal Computer e l'avvento di Internet, il quale ha di conseguenza contribuito alla diffusione dei computer.

Queste nuove tecnologie fanno si che si debba ripensare il ruolo dell'uomo nella società, la quale ad oggi può essere definita come una "società digitale" vista l'enorme incidenza dei media digitali nella vita quotidiana. L'uomo del terzo millennio si ritrova a svolgere molte azioni "online", e questo ha fatto si che si venissero a creare nuove fattispecie di reato che presentano il problema della localizzazione dell'illecito: il *cyberspazio* non ha confini, non ha luogo, è uno spazio immateriale in cui le informazioni circolano ad una velocità iperbolica e in cui tutto è facilmente accessibile da chiunque e in qualsiasi momento.

I crimini informatici trovano terreno fertile nel cyberspazio, sia per il fatto che è particolarmente complesso localizzare il reato, sia perché i cybercriminali possono facilmente nascondersi dietro l'anonimato e quindi rendersi difficilmente riconoscibili e rintracciabili.

Se le nuove tecnologie hanno portato dei benefici sotto certi punti di vista, al contempo hanno contribuito all'originarsi di nuove modalità devianti e criminali, oltre alla creazione nell'individuo di una distorta percezione della realtà, che lo porta ad assumere diverse personalità "virtuali" credendo di non incorrere in nessun rischio.

Dopo questa prima analisi sociologica del fenomeno, si è passati all'analisi della regolamentazione giuridica, spaziando dalla legislazione italiana a quella europea, descrivendo quindi in che modo vengono regolati i *cybercrimes*.

Nel nostro ordinamento l'introduzione dei reati informatici è avvenuta con la Legge n. 547 del 1993: il Legislatore ha preso consapevolezza del fatto che Internet e i computer hanno contribuito alla creazione di nuove forme di aggressione ai beni giuridici e che tali forme di aggressione necessitavano di una regolamentazione che prima era inesistente.

È necessario fronteggiare queste nuove minacce causate dal progresso tecnologico, e questo lo afferma anche l'Unione europea, la quale si è posta come obiettivo quello di combattere il crimine informatico cercando di coordinare gli Stati membri nell'adozione di misure che siano il più uniformi possibile fra loro.

Di fatto, attualmente la promozione della digitalizzazione e la guida alla trasformazione digitale sono fra le priorità principali dell'UE.

È stato opportuno fare riferimento alla Convenzione di Budapest quale primo accordo internazionale inerente i crimini informatici, considerato come il primo strumento giuridico internazionale nell'ambito dei cybercrimes, la quale ha come intento l'armonizzazione dei sistemi penali nazionali con riferimento a queste nuove forme di reato.

L'introduzione della disciplina concernente i reati informatici ha inevitabilmente fatto sorgere delle problematiche sia con riferimento al *locus commissi delicti*, sia per quanto riguarda questioni come l'individuazione del giudice competente o la localizzazione del *server* dal quale proviene l'azione criminosa: nell'elaborato sono stati riportati alcuni casi e le rispettive soluzioni, in modo tale da avere qualche esempio per comprendere come si è mossa la giurisdizione nel caso concreto.

L'ultimo capitolo è interamente centrato sulla governabilità del *cyberspazio*: si è affrontato il concetto di "*code is law*" con riferimento alla *lex informatica*, sostenendo la tesi di Maestri, il quale afferma che il diritto nel cyberspazio è veicolato tramite il codice e che a governare il cyberspazio sia proprio il codice, facendo così perdere centralità al diritto.

Si è accennato anche al dibattito fra i cyber-paternalisti e cyber-libertari per affrontare la questione sulla regolabilità del cyberspazio e cercare di capire se Internet possa essere in un qualche modo regolato oppure se tutto debba essere lasciato al libero arbitrio degli utenti.

Inoltre si è parlato di de-territorializzazione in qualità sia di caratteristica fondamentale che denota il cyberspazio sia di principale fonte di indebolimento del diritto tradizionale, e di principio di territorialità, quale argomento centrale di ogni riflessione compiuta nell'elaborato con riferimento ai reati commessi tramite un mezzo informatico.

La principale problematica che viene affrontata nell'elaborato riguarda l'applicazione del principio di territorialità, il quale viene ostacolato dall'elevato tasso di delocalizzazione dei reati informatici, evidenziando che la risposta a questo problema risulta differente da Stato a Stato, mancando tutt'ora una legislazione uniforme nel campo.

Alcuni studiosi sostengono che questa lacuna potrebbe essere colmata dalla creazione di una Costituzione propria del cyberspazio: anche questo è stato oggetto di studio nel presente elaborato, che ha di fatto l'obiettivo di fornire una visione completa delle principali problematiche e delle possibili soluzioni alla questione del principio di territorialità applicato alla criminalità informatica.

CAPITOLO 1 - CRIMINALITÀ INFORMATICA: ANALISI SOCIOLOGICA DEL FENOMENO

1. *L'avvento delle rivoluzioni industriali: i mutamenti sociali e culturali a seguito della Terza e della Quarta Rivoluzione industriale*

Da sempre il progresso tecnologico ha influenzato il modo in cui gli uomini hanno interagito fra loro, si pensi anche solo all'interfacciarsi di un individuo con una pietra scheggiata che gli permette di costruire oggetti o semplicemente di procurarsi cibo: questo può dirsi un primo esempio di interazione tra prodotti tecnologici e specie umana.

Abbiamo assistito nel corso dei secoli a varie rivoluzioni industriali, che hanno innanzitutto fatto si che in ambito economico l'agricoltura abbia ceduto il primato alle attività industriali: l'introduzione della macchina a vapore, l'utilizzo dell'elettricità, l'avvento dell'informatica, dell'elettronica e dell'Internet, sono tutte innovazioni che ci sono pervenute nel corso degli anni, che si stanno tutt'ora evolvendo e che hanno rivoluzionato sia il mondo del lavoro sia la società, i rapporti umani, il nostro modo di vedere e di pensare il mondo.

Concentrandoci maggiormente sulle ultime due rivoluzioni industriali, possiamo affermare che la Terza Rivoluzione Industriale ha portato ad una crescita esponenziale del settore informatico: l'invenzione del Personal Computer, attorno agli anni Settanta, ha cambiato radicalmente il nostro modo di vivere, facendo si che per moltissimi lavori non sia più necessaria la presenza fisica in un luogo ma basti avere a disposizione questo apparecchio di piccole dimensioni, ad oggi alla portata economica di tutti e pratico da trasportare in qualsiasi luogo. Conseguentemente all'avvento di Internet, una rete globale che permette di collegare più computer tra loro in tempo reale, la diffusione dei PC è aumentata esponenzialmente, rendendolo oggi uno strumento comune e a tratti "scontato".

Alcuni sostengono che la Terza Rivoluzione Industriale abbia dato inizio ad un processo di distruzione della vita: l'uomo è ormai superato, i soggetti della storia sono ora diventati la tecnologia, l'intelligenza artificiale e la cibernetica, protagonisti della

cosiddetta “Industria 4.0” (termine utilizzato per parlare della Quarta Rivoluzione Industriale, o meglio per indicare l’applicazione delle tecnologie smart in ambito manifatturiero[1]).

Questa Industria 4.0 è diretta conseguenza del processo di digitalizzazione, ed essere digitalizzati vuol dire saper rispondere alle esigenze di un mercato che è in continuo mutamento e che richiede adattamento da parte degli individui e, economicamente parlando, delle aziende. Le nuove tecnologie consentono una migliore gestione delle tempistiche e delle risorse, creando una rete virtuale in cui condividere informazioni interne ed esterne, il che migliora le performance aziendali. L’Internet Economy è infatti diventata la “colonna portante dell’economia globale”[2].

Le macchine sono ripetibili in serie, l’uomo no: l’uomo non è eterno e non potrà mai avere la caratteristica dell’eternità, a differenza di una macchina.

Inizia così a perdere importanza all’interno del sistema sociale, di fatto egli ha creato la macchina e ora quest’ultima sta prendendo il sopravvento su di lui, che si sente inadeguato, quasi antiquato[3]. L’uomo abbandona la visione ottimistica della tecnologia e inizia a perdere la fiducia nei confronti della modernità, avendo un’immagine angosciosa del futuro[4].

Con la Terza Rivoluzione Industriale iniziano a sollevarsi i primi problemi etici riguardo l’impatto della tecnologia sull’uomo, problemi che verranno poi accentuati dall’attuale rivoluzione di cui siamo protagonisti: la Quarta Rivoluzione industriale.

Quest’ultima affonda le sue radici negli anni Settanta e Ottanta del Novecento, anni in cui iniziano ad emergere innovazioni tecnologiche legate soprattutto alle *information tecgnologies* e alle rispettive ricadute. Sentiamo spesso parlare di robotica, smart city, intelligenza artificiale e iper-connessione, parole che sono entrate a seguito della Quarta Rivoluzione nello scenario quotidiano e che fanno riferimento ad un cambiamento non solo dell’economia ma anche della società. Sembra che discorsi di questo tipo tendano a dividere i sentimenti degli individui in due tipologie: quelli di tecno-entusiasmo e quelli

---

[1] Lazzeroni M., Zamperlin P., 2022. *La Quarta Rivoluzione Industriale tra Opportunità e Disuguaglianze*, FrancoAngeli s.r.l., Milano.

[2] Severino, P. 2019. *Standard globali in difesa della trasformazione digitale*, in *Il Sole 24 Ore*, 29 marzo, in https://www.ilsole24ore.com/art/standard-globali-difesa-trasformazione-digitale-ABZPmDjB.

[3] Campa, R. 2007. *Considerazioni sulla Terza Rivoluzione Industriale*, in *Il pensiero economico moderno*, Vol. 3, Pisa.

[4] Di Donato, M. 2022. *La Quarta Rivoluzione Industriale tra Opportunità e Disuguaglianze*, FrancoAngeli s.r.l., Milano.

di tecno-fobia. I portatori di sentimenti di tecno-entusiasmo tendono a considerare l'evoluzione tecnologica come strumento indispensabile per fattori come l'innalzamento della qualità di vita (sanità, ambiente, mobilità, ecc.), la crescita economica e il miglioramento delle condizioni di lavoro. Gli altri invece, "i tecno-fobici", hanno una visione più distopica dei rischi che possono emergere dall'evolversi della tecnologia, come le questioni etiche della sorveglianza e il capitalismo delle piattaforme[5], negativismo dovuto dal fatto che sono avvolti dall'incertezza di non riuscire a comprendere a fondo le caratteristiche e gli effetti sia negativi che positivi.

La Quarta rivoluzione ci ha in un certo senso tolto il nostro autoconvincimento di essere unici: citando Floridi, siamo organismi informazionali connessi l'uno con l'altro e facciamo parte di un ambiente informazionale, che condividiamo con altri agenti informazionali (siano essi naturali o artificiali) che elaborano informazioni in modo autonomo. Sempre più di frequente facciamo affidamento su applicazioni munite di intelligenza artificiale per svolgere dei compiti che ci risulterebbe impossibile concludere senza ulteriori risorse oltre all'intelligenza umana[6].

Oggi l'esperienza conseguita dal web è inserita nell'*everyday life*, ovvero nella vita di ogni giorno, così come le altre esperienze quotidiane.

Siamo entrati nell'era digitale ben prima del 2020, ma a partire da questo anno in poi abbiamo assistito ad una inquietante ed inaspettata accelerazione dell'intrecciarsi delle tecnologie digitali con la vita quotidiana. Infatti, il periodo del lockdown dovuto alla pandemia da Covid-19, ha fatto si che digitalizzazione e pratiche digitali venissero utilizzate come mai prima di allora in maniera così massiccia, a causa della privazione del movimento nello spazio pubblico. I dati di una ricerca condotta dall'Agence France-Presse mostrano che al 30 marzo 2020 oltre 3,38 miliardi di persone si trovavano chiusi nelle proprie abitazioni o comunque obbligati a sottostare a limitazioni di movimento: in sostanza il 43% degli abitanti del mondo, 4 persone su 10[7].

---

[5] Lazzeroni M., Albanese V., 2022. *La Quarta Rivoluzione Industriale tra Opportunità e Disuguaglianze*, FrancoAngeli s.r.l., Milano.

[6] Floridi, L. 2017. *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano.

[7] Benanti P., Maffettone S., 2021. "*Sostenibilità D". Le conseguenze della rivoluzione digitale nelle nostre vite*, in *Il Mulino – Rivisteweb*, Fascicolo 2, pp. 192-206.

Gli individui si sono trovati a dover ripensare lo spazio, vivendo come spazio di eccezione quello esterno e trasformando per esempio quello interno nel luogo di lavoro (da qui l'espressione "smartworking")[8].

Questo periodo da poco passato ci ha portati oggi, ormai nel post-pandemia, a confrontarci con una massiccia presenza delle tecnologie digitali in tutti i contesti sociali della quotidianità, dal lavoro, all'istruzione, ai servizi, tanto che informatica e robotica sono ad oggi in grado di svolgere compiti materiali, sostituendosi così alle persone fisiche.

Citando un esempio riportato da Moro[9], si pensi a quelle attività di deposito e/o notifica degli atti, come anche alla ricerca di precedenti giurisprudenziali: parliamo di attività che possono essere effettivamente svolte da organismi informatici.

Floridi ci insegna che la nostra epoca è la fine della storia e l'inizio dell'iperstoria: la sollecitazione a ripensare in modo sempre più tecnologicizzato il presente e il futuro, richiede l'intervento di una nuova filosofia dell'informazione che sia in grado di trattare qualsiasi aspetto della nostra situazione iper-storica.

Nell'iper-storia le protagoniste sono le Information and Communication Technologies che registrando, trasmettendo e processando le informazioni sempre più con autonomia, risultano essere le più potenti tecnologie del sé alle quali siamo mai stati esposti[10]. Un cauto ottimismo nei confronti di queste nuove tecnologie può essere giustificato dal fatto che queste siano anche in grado di diminuire l'ambito dei rischi e renderli maggiormente gestibili: Floridi sostiene che le ICT siano capaci di aiutare l'uomo nella lotta contro la distruzione, la devastazione, l'impoverimento e lo spreco delle risorse sia naturali che umane, oltre che storico-culturali. L'Autore parla delle ICT come un "prezioso alleato" in ciò che egli ha definito come "ambientalismo sintetico o digitale".

Non siamo e non saremo mai più in grado di disconnetterci dalle ICT: dobbiamo ripensare il nostro ruolo nella "società digitale" in cui viviamo, dove i media digitali sembrano essere oltre alla maggiore espressione culturale, anche fra i maggiori agenti di

[8] Albanese, V. 2022. *La Quarta Rivoluzione Industriale tra Opportunità e Disuguaglianze*, FrancoAngeli s.r.l., Milano.

[9] Moro, P. 2019. *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *MediaLaws – Rivista di diritto dei media*, pp. 12-22.

[10] Floridi, L. 2017. *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano.

socializzazione, e dove l'analfabetismo digitale sta diventando un problema a causa dei suoi effetti di divisione sociale[11].

Sarra ci dice che la tecnica è *accrescimento*, è proiettata verso un costante superamento delle sue realizzazioni storiche: la tecnica deve evolversi continuamente per evitare che ci si trovi in una situazione di incapacità di soddisfare le esigenze che inevitabilmente si vengono a creare dopo ogni raggiungimento: l'uomo non può permettersi di evitare questo accrescimento[12].

Sono state proprio le invenzioni culturali e scientifiche dell'era post-industriale causate dalla rivoluzione digito-globale ad incrementare una "*new crime's way*" molto complessa e ad aprire nuove problematiche in merito al *technology risk assessment*[13].

L'esplosiva e continua crescita delle tecnologie informatiche non calibrata da un'adeguata regolamentazione giuridica ha contribuito a creare uno spazio grigio, in cui è possibile agire per scopi antisociali rimanendo impuniti[14].

2. *Le ragioni sociali alla base della nascita della criminalità informatica nel Cyberspazio*

L'avvento di Internet, la cosiddetta "Rete delle reti[15]", principale causa della rivoluzione globale da cui siamo avvolti, ha prodotto notevoli cambiamenti nel contesto sociale: la maggior parte delle attività che normalmente venivano svolte "*off-line*", l'uomo del terzo millennio si ritrova a svolgerle "*online*", costretto così ad adeguarsi ad una società in cui le tecnologie si muovono più velocemente di essa stessa[16].

---

[11] Benanti P., Maffettone S., 2021. "*Sostenibilità D". Le conseguenze della rivoluzione digitale nelle nostre vite*, in *Il Mulino – Rivisteweb*, Fascicolo 2, pp. 192-206.

[12] Sarra, C. 2018. "*Iper positività": la riduzione del giuridicamente lecito al tecnicamente possibile nella società dell'informazione*, in *JusQuid – sezione scientifica*, pp. 95-122.

[13] Di Fede, C. 2004. *La Criminalità informatica: un'analisi socio-criminologica*, in *Tecnologie dell'Informazione e Comportamenti Devianti*, LED Edizioni Universitarie.

[14] Vigneri, F. 2019. *Brevi considerazioni sulla natura e sulle caratteristiche dello spazio cibernetico*, in *Internazionale*, 10 ottobre, in http://www.salvisjuribus.it/brevi-considerazioni-sulla-natura-e-sulle-caratteristiche-dello-spazio-cibernetico/.

[15] Vulpiani, D. 2007. *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. I, pp. 1-9.

[16] Di Donato, M. 2022. *La Quarta Rivoluzione Industriale tra Opportunità e Disuguaglianze*, FrancoAngeli s.r.l., Milano.

L'avvento di nuove tecnologie di comunicazione ha comportato notevoli cambiamenti in merito alla diffusione dell'informazione: ampiezza e velocità sono le colonne portanti del cambiamento che caratterizza l'informazione nell'era odierna, la quale è in grado di raggiungere con una velocità iperbolica un grande numero di soggetti che distano tra loro migliaia di chilometri[17].

Ad oggi sono circa 5,2 miliardi gli utenti che si trovano connessi alla rete Internet, e ogni giorno oltre un milione di nuovi utenti si inserisce nel mondo del web, ciò significa che circa il 65% della popolazione globale è online[18].

Internet non elimina le frontiere, ma bensì crea un mondo in cui ognuno vive su un confine in cui passare in un'altra "giurisdizione" non richiede sforzo e non ha vincoli[19].

La tecnologia informatica, pur presentando molteplici opportunità di sviluppo positive sia nell'ambito sociale che su quello economico-culturale, delinea una nuova via rappresentata da un ambiente intangibile che apre le porte ad un nuovo locus commissi delicti: il cyberspazio, anche detto *spazio-non-spazio*, che ha caratteristiche assai distinte da quelle dello spazio fisico, che invece ben conosciamo; costituisce una dimensione immateriale, delimitata da confini non percettibili in cui i dati informatici viaggiano in modo rapido e diffuso.

Il termine "cyberspazio" è stato coniato per la prima volta nel 1984 dallo scrittore canadese William Gibson, il quale nel romanzo dal titolo "Neuromante" riferisce di uno spazio digitale e navigabile proprio con questi termini: "Cyberspazio. Un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici. Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano". Sebbene Gibson ne parlò per la prima volta, egli stesso affermò comunque che anche se lo vide sorgere mentre scriveva, nemmeno per lui il termine coniato aveva un significato specifico. Fu il giornalista e scrittore Bruce Sterling che riprendendo il termine da Gibson contribuì a renderlo

[17] Vigneri, F. 2018. *I nuovi scenari criminali: introduzione al fenomeno del cybercrime*, in *Penale*, 17 dicembre, in http://www.salvisjuribus.it/i-nuovi-scenari-criminali-introduzione-al-fenomeno-del-cybercrime/.

[18] Tonellotto, M. 2022. *Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. XVI, pp. 7-19.

[19] Kobrin, S. J. 2001. *Territoriality and the Governance of Cyberspace*, in *Journal of International Business Studies*, Vol. 32, pp. 687-704.

popolare, descrivendo il "cyberspazio" come "un luogo espanso, un vasto e fiorente paesaggio elettronico". Citando le parole di Sterling, "dagli anni Sessanta, il mondo del telefono è divenuto ibrido con i computer e la televisione, e sebbene non vi sia ancora alcuna sostanza di cyberspazio, nulla che si possa maneggiare, esso ora ha uno strano tipo di fisicità. È buonsenso oggi parlare di cyberspazio come un luogo a sé stante"[20].

Si può dire essere uno spazio caratterizzato da un "diluvio informazionale[21]" in costante sviluppo, che risulta raggiungibile da chiunque sia dotato di un dispositivo in grado di navigare in Internet, il tutto a basso costo e in qualsiasi momento.

Nessuno si trova realmente nel cyberspazio: la metafora del *cyberspace as place* (tradotto, cyberspazio come luogo) viene sconfessata dalla consapevolezza che Internet è semplicemente un protocollo, cioè una parte del "*code*" che permette agli utenti di trasmettere dati tra computer attraverso i network esistenti.

Indubbiamente ciò che più caratterizza il cyberspazio, dopo l'avvicinamento tra individui separati fisicamente da lunghe distanze, è il venir meno della territorialità, che è carattere intrinseco di un ordinamento giuridico: per questo motivo non è possibile delimitare l'ambito di operatività delle norme statali, il che risulta essere una delle maggiori problematiche da affrontare a livello giurisprudenziale. Possiamo affermare che il *cyberspazio* distrugge il significato di localizzazione fisica.

I confini territoriali vengono ignorati dall'Internet, motivo per cui risulta indispensabile per gli ordinamenti giuridici tentare di delimitare uno spazio sul quale esercitare la propria sovranità, in modo tale che al soggetto attivo, celato dietro l'anonimato, risulti difficoltoso avvalersi dell'impunità offerta dalle leggi del luogo in cui agisce[22].

Assistiamo ogni giorno ad una sorta di sgretolamento delle categorie giuridiche tradizionali dovuto alle continue innovazioni tecnologiche: il diritto nel mondo digitale viene "tecnologicizzato", la territorialità viene come sostituita dalla spazialità e Internet risulta ad oggi essere il più grande spazio pubblico che il globo abbia mai conosciuto[23], spazio all'interno del quale i singoli utenti possono diventare vittime e autori di fatti criminosi, tentando di nascondersi dietro all'anonimato e alla difficoltà nel localizzare

---

[20] Rocca, D. A. 2011. *Opportunità e rischi del "cyberspazio"*, in *Il Piacere della Cultura, Web e Nuove Tecnologie*, 22 aprile, in https://www.lucidamente.com/opportunita-e-rischi-del-cyberspazio/.

[21] Forte, F. 2016. *Il cyberspazio tra governamentalità e digitalità*, in *La Deleuziana – Rivista Online di Filosofia*, n. 3, pp. 87-101.

[22] Seminara, S., *Locus commissi delicti, giurisdizione e competenza nel cyberspazio*.

[23] Maestri, E. 2017. *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 15-26.

l'illecito commesso. Di fatto, il Cyberspace è caratterizzato da una elevata potenzialità criminale, dovuta da caratteri quali immediatezza degli effetti, semplice accessibilità, anonimato, illimitata diffusione dei contenuti; la lotta al Cybercrime, riferendoci a questo anche con il termine "reato cibernetico", è un campo ancora in fase di studio e di necessario continuo aggiornamento[24].

Gli strumenti informatici da un lato hanno contribuito a porre in essere dei fatti già costituenti reato con nuove modalità (per esempio la diffamazione a mezzo internet su un quotidiano online o su un social network), dall'altro lato hanno dato origine a dei nuovi fenomeni criminali che, pregiudicando dei beni giuridici meritevoli di tutela, hanno portato il legislatore a dover necessariamente introdurre nuove fattispecie penali incriminatrici (pensiamo per esempio all'introduzione dell'art. 615-ter: "Accesso abusivo a un sistema informatico o telematico").

A causa dell'espansione dell'utilizzo dell'ambiente cyber per compiere condotte criminali, e quindi a scopo illegale, tendiamo ad associare il concetto di cyberspace più ad un'idea di rischio e minaccia invece che di opportunità.

La tecnologia ha trasformato il modo di pensare e agire dell'uomo: ha assunto un ruolo di primo piano tra le forze generatrici dei cambiamenti socio-culturali, e in questo contesto i crimini informatici rappresentano la principale materializzazione di questa nuova complessità. Si tratta di una forma di crimine transnazionale il cui accesso e la cui conservazione sono facilmente trasferiti a livello globale e il cui controllo e regolamentazione impongono un'elevata difficoltà e complessità, ed è per questo che mai come ora è richiesta una forte cooperazione internazionale fra i diversi Paesi.

L'introduzione di nuove forme di reato si basa sulla sentita esigenza di tutela di nuovi beni giuridici, per esempio il domicilio informatico o l'intangibilità informatica, ritenuti meritevoli di tutela nell'ordinamento penale[25].

I confini territoriali che delimitano gli Stati perdono sempre più forza e il monopolio statale sulla creazione delle norme e la sua forza autoritaria si stanno indebolendo: l'aumento dei crimini globali richiede una nuova risposta internazionale[26].

---

[24] Panattoni, B. 2019. *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online*, in *Diritto Penale Contemporaneo - Rivista Trimestrale*, Vol. 2, pp. 35-52.

[25] Battaglia, S. 2013. *Criminalità informatica al tempo di internet: rapporti tra phishing e riciclaggio*, in *Altalex*, 18 settembre, in https://www.altalex.com/documents/news/2014/03/28/criminalita-informatica-al-tempo-di-internet-rapporti-tra-phishing-e-riciclaggio.

Come afferma Floridi, la generazione del terzo millennio si sta cimentando nel passaggio dalla storia all'iperstoria: le società dell'informazione avanzate, sempre più notevolmente dipendono dalle ICT, Information and Communication Technologies, per il loro consueto funzionamento e potenziamento. Inoltre, solo "una società che vive nell'età dell'iperstoria può essere minacciata in termini informazionali con un cyber-attacco[27]": la criminalità organizzata si sta adeguando alla rivoluzione digitale e le attività compiute dai criminali informatici sono in costante crescita e sempre più inarrestabili.

Il cyberindividuo deve assumersi la responsabilità di controllare consapevolmente il progresso tecnologico, cercando di guidarlo verso un costante miglioramento delle proprie e altrui condizioni di vita.

3. *Definizione di crimine informatico e individuazione di autori e vittime della criminalità informatica*

L'utilizzo dell'alta tecnologia informatica ha portato nel corso degli ultimi decenni alla formazione di un nuovo profilo di criminalità: i crimini informatici, anche conosciuti come "*computer crime*" o "*cybercrime*".

Risulta ancora difficile riuscire a dare una definizione esaustiva di criminalità informatica e la difficoltà di interpretazione ha ricadute sulle norme giuridiche, le quali necessitano di continui aggiustamenti.

Esperti del settore hanno tentato di dare una possibile definizione di crimine informatico, anche se non si è mai giunti ad una univoca, probabilmente a causa anche dell'eterogeneità delle modalità con cui può essere compiuto: prendiamo come punto di riferimento la definizione di Ceccacci, che afferma che "il crimine informatico rappresenta qualsiasi atto o fatto contrario alle norme penali, nel quale il *computer* è

---

[26] Leonhardt dos Santos, D. 2019. *A territorialidade no contexto da criminalidade global: considerações sobre a influência do ciberespaço na delimitação jurisdiccional*, in *Rev. Bras. De Direito Processual Penal*, Porto Alegre, Vol. 5, pp. 597-622.

[27] Floridi, L. 2017. *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano.

stato coinvolto come strumento, simbolo od oggetto del fatto[28]". Provando ad essere ancora più esaustivi, possiamo dire che il *computer crime* può comprendere tutti quei casi in cui un qualsiasi mezzo telematico si intromette fra autore e vittima del reato, rappresentando il mezzo principale di esecuzione della condotta criminale e modificando la percezione della gravità del crimine stesso[29].

Facendo riferimento al trattato del Consiglio d'Europa sulla criminalità informatica, in questo il termine "cyber crime" viene utilizzato per definire "reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici", che possono manifestarsi con attività quali: l'"accesso illegale" (art. 2), le "intercettazioni illegali" (art. 3), "Data & System Interference" (artt. 4-5), "uso improprio di dispositivi" (art. 6), "frode informatica e falso" (artt. 7-8), "reati connessi alla pornografia infantile" (art. 9), "reati connessi a violazioni del diritto d'autore e dei diritti connessi" (art. 10)[30].

Un'altra parte della dottrina suggerisce invece una definizione ancora più ampia, includendo anche attività criminose quali la frode, l'accesso non autorizzato, la pedopornografia e il pedinamento informatico (o "cyberstalking")[31].

Le concrete dimensioni del fenomeno sono di difficile quantificazione, ma possiamo affermare che i dati siano in costante incremento seguendo l'ondata di informatizzazione dei Paesi.

Volendo fornire qualche dato statistico, l'Osservatorio Cybersecurity di Exprivia ha osservato che nel 2022 in Italia sono stati registrati 2.600 fenomeni connessi al crimine informatico, ciò significa il doppio del 2021 e oltre il quadruplo del 2020: il numero di incidenti informatici, cioè quella parte di attacchi andati a buon fine, ha oltrepassato il numero degli attacchi; questo incremento esponenziale è stato causato sia dalle sempre più sofisticate tecniche usate dagli hacker, sia dalla scarsa consapevolezza da parte di imprese e dei cittadini in merito ai rischi legati alla rete[32].

---

[28] Ceccacci, G. 1994. *Computer crimes*, Fag, Milano.

[29] Di Fede C., Corradini I., 2004. *La Criminalità informatica: un'analisi socio-criminologica*, in *Tecnologie dell'Informazione e Comportamenti Devianti*, LED Edizioni Universitarie.

[30] Aterno, *Sull'accesso abusivo a un sistema informatico o telematico*, in Cass. Pen., 2000, p. 2995 ss.

[31] Battaglia, S. 2013. *Criminalità informatica al tempo di internet: rapporti tra phishing e riciclaggio*, in *Altalex*, 18 settembre, in https://www.altalex.com/documents/news/2014/03/28/criminalita-informatica-al-tempo-di-internet-rapporti-tra-phishing-e-riciclaggio.

[32] Licata P. 2023. *Cybercrime, in Italia il 70% degli attacchi mirato al furto dei dati*, in *Network Digital 360*, 14 febbraio, in https://www.corrierecomunicazioni.it/cyber-security/cybercrime-in-italia-il-70-degli-attacchi-mirato-al-furto-dei-dati/.

I nuovi crimini informatici trovano terreno fertile nel cyberspazio e sono principalmente incentrati sul furto di identità e su settori come i servizi bancari online e il commercio elettronico, hanno come punto in comune l'appropriazione indebita dei dati sensibili delle persone, quindi la violazione della privacy dell'individuo.

Pensando alla figura del criminale informatico ci si immagina un soggetto che vive in una sorta di mondo nascosto, anonimo, lontano dalla società e distante dalla realtà, mentre invece in molti casi egli non è né un disadattato né un emarginato, ma anzi un individuo perfettamente integrato tanto nell'ambiente professionale quanto in quello sociale[33].

Da alcuni studi è emerso che il cyber criminale ha un'istruzione medio-alta, manifesta una ridotta percezione del crimine e un'ottima capacità di premeditazione ed organizzazione, inoltre non sempre presenta un comportamento violento o antisociale. Operando in solitudine, accresce la sua autostima nello svolgere quello che da lui è visto come un "gioco eccitante"[34].

I vecchi cracker o hacker non risultano più essere i principali artefici dei crimini informatici, ma appaiono più come meri prestatori d'opera, a cui o vengono affidati compiti, per esempio la creazione di virus, oppure il diretto inserimento nelle nuove imprese criminali: volendo fare un paragone, possiamo raffigurare la nuova criminalità informatica come una sorta di impresa in cui boss con capacità manageriali accentuate reclutano e ingaggiano tecnici esperti nella creazione di virus o malware o per esempio nell'allestimento di siti clone, al fine di eseguire attività informatiche illecite, il tutto compensato poi in denaro[35]. Essendo il cyberspace caratterizzato dalla possibilità di nascondersi dietro l'anonimato, dando in tal modo ai criminali la possibilità di celarsi dietro numerosi nascondigli sia nel mondo reale sia nella rete stessa, spesso accade che i soggetti demandati al compimento di queste azioni criminose non sappiano nemmeno chi sono i loro leader.

Ai fini delle analisi delle dinamiche dei processi di vittimizzazione in ambiente virtuale e quindi dell'individuazione di chi è più esposto alla vittimizzazione, bisogna tener

[33] Marotta, G. 2012. *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. VI, pp. 94-106.

[34] Battaglia, S. 2013. *Criminalità informatica al tempo di internet: rapporti tra phishing e riciclaggio*, in *Altalex*, 18 settembre, in https://www.altalex.com/documents/news/2014/03/28/criminalita-informatica-al-tempo-di-internet-rapporti-tra-phishing-e-riciclaggio.

[35] Apruzzese, A. 2010. *Autori e vittime nella criminalità informatica*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. III-IV, pp. 101-106.

conto di alcuni fattori come l'età, il genere, l'evento criminale e l'attribuzione delle responsabilità dell'evento. Alcune ricerche mostrano che fra i soggetti più esposti alla vittimizzazione vi sono le donne e i minori; riguardo l'evento invece bisogna sottolineare che spesso il rapporto autore-vittima sorge da contatti tra sconosciuti e non necessariamente da precedenti relazioni affettive o di mera conoscenza.

Parlando di vittimizzazione online, possiamo distinguere tre categorie di vittime: quelle adescate online e poi abusate nel contesto reale; quelle abusate nel proprio ambiente relazionale-sociale le cui immagini di abusi vengono diffuse tramite i new-media; quelle che on-line vengono sia adescate che abusate[36].

I soggetti più propensi a cadere nelle trappole dei cybercriminali sono emotivamente instabili, individui che si trovano sul web in ricerca di attenzione sociale per "sentirsi qualcuno" o semplicemente per contrastare la solitudine, che finiscono ingenuamente per fornire un proprio identikit composto da dati sensibili, utilizzati poi dagli autori della condotta criminosa per colpire.

Le caratteristiche comuni che più spiccano fra le vittime di crimini informatici sono l'uso della rete con regolarità, il fatto di essere sicuri di sé stessi, l'utilizzo di più dispositivi mobili per connettersi sia da casa sia in contesti al di fuori dell'abitazione. Anche aspetti molto comuni come l'utilizzo di un dispositivo elettronico per lo streaming e l'uso abitudinario di piattaforme online per gli acquisti sembrano essere due fattori che contribuiscono alla propensione all'essere vittime di crimini informatici.

Il luogo dove si consumano i reati informatici raramente si identifica con un luogo fisico, dato che la condotta criminosa si verifica nel cyberspazio: la caratteristica della transnazionalità, propria del cyberspace, fa si che le nuove imprese criminali non conoscano più barriere o limiti territoriali, rendendo così indispensabile una forte normativa di contrasto e di sanzione nei confronti dei cyber-criminali.

Il modo di agire dei cybercriminali è inoltre caratterizzato dal criterio dell'ubiquità, ovvero la facoltà di essere presenti in più posti contemporaneamente, e questo fattore contribuisce a far sì che l'individuazione del *locus commissi delicti* risulti complessa.

Un monitor connesso è un proiettore, è "una mano direttamente nel mondo", e sta a noi, soggetti parte di una collettività, favorire un'educazione all'utilizzo consapevole e

[36] Marotta, G. 2012. *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. VI, pp. 94-106.

razionale di questi dispositivi, per far si che questo mondo virtuale non si trasformi in un precipizio in cui possono cadere vittime la cui privacy viene violata.

4. *Il concetto di devianza informatica alla luce della nozione di condotta digitale*

L'uomo si adatta costantemente alle modifiche che l'ambiente subisce e queste risposte adattive, a seguito di un lasso di tempo più o meno lungo, tendono a stabilizzarsi in caratteristiche strutturali. In questa fase storica il sistema nervoso degli individui si trova costretto ad adattarsi e sintonizzarsi a nuove modalità di interazione con gli altri esseri umani, con nuovi oggetti, con lo spazio fisico nel quale si trova avvolto e talvolta con il proprio corpo: l'individuo si trova sommerso da una fitta rete di comunicazioni che in particolari condizioni pare prendere vita propria[37].

Se le nuove tecnologie hanno prodotto notevoli effetti positivi, allo stesso modo hanno inevitabilmente contribuito all'affermarsi di nuove modalità devianti e criminali.

Con l'avvento di Internet, l'informazione è diventata l'elemento chiave della società: sviluppo, trasmissione ed elaborazione delle informazioni divengono elementi base di produttività e potere[38].

Ad oggi la prevalenza della cosiddetta "*technology culture*" ha fatto sorgere l'importanza di quelli che sono gli elementi astratti del processo comunicativo, rivoluzionando le modalità di interazione fra gli individui. Stiamo assistendo ad una riduzione dei rapporti *face to face* e quello che consideriamo spazio pubblico in cui socializzare con gli altri sta traslando oggi dal mondo reale al mondo virtuale: alcuni lo considerano "settimo continente" questo mondo virtuale che si sovrappone a quello tradizionale, nel quale la distorta percezione di noi stessi e della collettività contribuisce alla definizione di condotte devianti e criminali[39].

Nell'era attuale dell'*Information Technology* pare che non si riesca ad evitare di essere martellati dalle informazioni. L'uso eccessivo della tecnologia ha portato all'insorgere

---

[37] Strano, M. 2001. *Relazioni digitali e comportamenti devianti*, Relazione al convegno "Psichiatria informatica e telemedicina. Realtà e prospettive nel campo dell'assistenza della formazione", 29 marzo, Velletri.

[38] Blengino, C. 2009. *La devianza informatica tra crimini e diritti: un'analisi sociogiuridica*, Carocci, Roma.

[39] Di Fede C., Corradini I., 2004. *La Criminalità informatica: un'analisi socio-criminologica*, in *Tecnologie dell'Informazione e Comportamenti Devianti*, LED Edizioni Universitarie.

di nuove psicopatologie e di nuovi modelli socio-comportamentali, oltre a nuovi processi comunicativi che si orientano più verso una trasmissione di "segni" piuttosto che ad una trasmissione di gesti ed espressioni (pensiamo all'utilizzo delle emoticon nello scambio di messaggi).

Internet altro non è che una catena di connessioni telefoniche (Blumer 1969, Mead 1972) e l'individuazione e la conseguente definizione di atteggiamenti devianti nella nostra società sembrano rispondere ad un'esigenza di introduzione di confini morali[40].

La generazione Zeta è ormai diventata dipendente da tutto ciò che è tecnologico: con il termine *net addiction* si fa riferimento proprio alle dipendenze tecnologiche, le quali coinvolgono l'individuo nella sua complessità, soprattutto nella sfera professionale, relazionale ed economica[41]. La Young[42] ha fornito un indice dei principali segni clinici ai fini della diagnosi della dipendenza da Internet, e fra questi troviamo il bisogno di utilizzare Internet sempre più a lungo termine per giungere al soddisfacimento, utilizzarlo come strumento per fuggire dai problemi, l'incapacità di controllare il proprio utilizzo della rete e il sentimento di irritazione mentre si tenta di interrompere l'utilizzo di Internet. L'uso patologico di Internet può compromettere la vita del *net slave* (schiavo della rete) in molti contesti, come ad esempio il lavoro e le relazioni personali, comportando una scarsa concentrazione mentale del soggetto.

La grande quantità di informazioni e di dati molto spesso inattendibili o non precisi che si trovano in rete, sono in grado di esporre i più giovani a rischi di sovraccarico cognitivo, oltre al disorientamento e all'inganno, per questo motivo è necessario educarli all'utilizzo critico delle informazioni digitali, infatti solo così si potrà favorire lo sviluppo di competenze cognitive che siano adeguate nei soggetti qui considerati[43].

Il cyberspazio dovrebbe essere inteso non come il luogo dove vivere le proprie emozioni, ma come un complemento della realtà: nella *net addiction* può sorgere il problema della "dissociazione", ossia il caso in cui non si riesce ad integrare la vita

---

[40] Blengino, C. 2009. *La devianza informatica tra crimini e diritti: un'analisi sociogiuridica*, Carocci, Roma.

[41] Galdieri P., Corradini I., 2004. *La Criminalità informatica: un'analisi socio-criminologica*, in *Tecnologie dell'Informazione e Comportamenti Devianti*, LED Edizioni Universitarie.

[42] K. Young, Center for on-line addiction.

[43] Rocca, D. A. 2011. *Opportunità e rischi del "cyberspazio"*, in *Il Piacere della Cultura, Web e Nuove Tecnologie*, 22 aprile, in https://www.lucidamente.com/opportunita-e-rischi-del-cyberspazio/.

reale e la vita virtuale, e questo può comportare ad un'alterazione dell'equilibrio emotivo del soggetto[44].

Per i giovani più timidi indubbiamente queste nuove tecnologie rappresentano una forma alternativa di socializzazione, seppur falsata ma comunque meno sofferta rispetto a quella della vita reale. Questa categoria di soggetti è però altamente esposta oltre al rischio dell'isolamento relazionale, anche all'insorgere di vere e proprie dipendenze: *Internet Addiction Disorder* (IAD), *Pathological Internet Use* (PIU) o *Internet Related Psychopathology* (IRP) sono considerati come forme di abuso-dipendenza da Internet sullo stesso piano di alcoolismo e tossicodipendenza, possono infatti provocare problemi socio-economici, isolamento, astinenza e problemi sul luogo di lavoro. Possiamo quindi affermare che l'utilizzo della rete e quindi la protezione della individualità dietro ad un monitor, ha il potenziale di causare l'insorgenza di disturbi psicopatologici[45].

Blengino[46] sostiene che il processo di costruzione della devianza informatica sia segnato da tre principali tappe: la prima è la scoperta dell'abuso informatico; la seconda concerne la definizione giuridica dei reati informatici; la terza invece coincide con la demonizzazione degli hacker. L'identità di deviante viene infatti attribuita prevalentemente all'hacker.

Gli studiosi di Criminologia si ritrovano in questo inizio di secolo a doversi confrontare con nuovi modi di comunicare e interagire, legati per lo più allo sviluppo e diffusione di tecnologie informatiche e anche alla nascita di nuove forme criminali (*computer crime*).

Parlando dell'influenza del digitale sul crimine, si osserva in certi soggetti una difficoltà nel processo di identificazione del limite che separa la realtà virtuale o nella dinamicità del tornare alla situazione reale a seguito di una lunga permanenza nella fase di virtualità: questa difficoltà è rilevante nel campo della Criminologia soprattutto nello studio delle fasi di percezione, distinzione, valutazione da parte del cybercriminale delle conseguenze provocate dal suo comportamento; la mente dell'autore di un crimine è

---

[44] Galdieri P., Corradini I., 2004. *La Criminalità informatica: un'analisi socio-criminologica*, in *Tecnologie dell'Informazione e Comportamenti Devianti*, LED Edizioni Universitarie.

[45] Marotta, G. 2012. *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. VI, pp. 94-106.

[46] Blengino, C. 2009. *La devianza informatica tra crimini e diritti: un'analisi sociogiuridica*, Carocci, Roma.

quindi avvolta da una dispercezione delle ripercussioni delle proprie azioni, il che lo porta ad esercitare una condotta deviante e quindi a violare le leggi[47].

Il criminale informatico spesso opera da solo con il proprio dispositivo elettronico, che sia il PC o lo smartphone, e non è in grado di capacitarsi del fatto che la sua condotta in quel momento può essere assimilata penalmente all'attività del rapinatore di strada[48].

Gli individui nel settimo continente sono liberi di assumere identità false ed immaginarie, con la possibilità di assumere diverse personalità e di non incorrere nel rischio di essere smascherati. Online questi soggetti si sentono al sicuro, protetti da uno schermo, credono di essere in una sorta di "mondo sicuro" dove tutti sono uguali e dove ci si può relazionare gli uni con gli altri senza l'ansia che si può invece avere nella vita reale, *face to face*. Il cyberspazio diventa così l'unica realtà di vita.

[47] Strano, M. 2001. *Relazioni digitali e comportamenti devianti*, Relazione al convegno "Psichiatria informatica e telemedicina. Realtà e prospettive nel campo dell'assistenza della formazione", 29 marzo, Velletri.

[48] Battaglia, S. 2013. *Criminalità informatica al tempo di internet: rapporti tra phishing e riciclaggio*, in *Altalex*, 18 settembre, in https://www.altalex.com/documents/news/2014/03/28/criminalita-informatica-al-tempo-di-internet-rapporti-tra-phishing-e-riciclaggio.

CAPITOLO 2 - LA REGOLAMENTAZIONE GIURIDICA DEI CYBERCRIMES A LIVELLO ITALIANO ED EUROPEO

1. *Introduzione dei reati informatici nell'ordinamento italiano: la Legge 547/1993*

Il computer è divenuto strumento-oggetto di attività illecita: considerando che nel nostro diritto penale vige il divieto di applicazione analogica della norma e che viene qualificato come reato solo quello che viene espressamente previsto dalla legge come tale, si è resa indispensabile l'introduzione dei reati informatici nel nostro ordinamento, in modo tale che il diritto penale si potesse adeguare ai casi in cui i reati fossero commessi a mezzo di computer oppure a danno dei sistemi informatici[49].

Alla base della promulgazione della legge che ha introdotto nel nostro ordinamento i crimini informatici, ci sono la necessità di predisporre una tutela giuridica adeguata a fronteggiare la diffusione di illeciti connessi alle nuove tecnologie e l'esigenza di equiparare il nostro diritto positivo a quello degli ordinamenti stranieri[50].

Prima dell'entrata in vigore della Legge n. 547, la magistratura italiana ha incontrato difficoltà nel fronteggiare le nuove condotte criminose: per citarne una, facciamo riferimento alla casistica delle truffe eseguite mediante l'alterazione del funzionamento dei sistemi di trasferimenti elettronici dei fondi, di solito prive dell'elemento degli artifizi e raggiri ai fini di indurre in errore una persona, ovvero elemento costitutivo fra i più caratteristici per l'individuazione del reato di truffa comune[51].

Come fondamento dell'intervento normativo ad opera del Legislatore con la Legge 23 dicembre 1993, n.547 vi è la consapevolezza della pericolosità delle nuove forme di aggressione ai beni giuridici, oltre che alle numerose difficoltà alle quali la giurisprudenza è andata incontro nell'operazione di estensione a questi casi delle previsioni di reato già presenti nell'ordinamento.

---

[49] Ruffilli, C. 2020. *I reati informatici e l'evoluzione del concetto di materialità*, in *Penale*, 15 luglio, in http://www.salvisjuribus.it/i-reati-informatici-e-levoluzione-del-concetto-di-materialita/.

[50] Del Re, C. 2009. *Formazione di un nuovo fenomeno criminale: i reati informatici. La frode informatica*, Edizioni Polistampa, Firenze.

[51] Amore, S. 2006. *Internet ed il diritto penale. I crimini informatici: dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Halley Editrice.

Le nuove fattispecie sono state elaborate sulla base del modello dei reati già presenti e, visto il mancato accoglimento dell'idea di creare un nuovo titolo del Codice Penale che fosse dedicato in modo specifico ai reati informatici, sono state poste nell'ambito della tradizionale sistematica del codice Rocco[52]. Prevalse la volontà di ricondurre i nuovi reati alle figure già esistenti all'apparenza più assimilabili a loro prevalentemente nella convinzione che data la particolarità della materia, questa non costituisse una sufficiente ragione per far si che si procedesse alla configurazione di uno specifico titolo dedicato[53].
Tale Legge, nominata "*Modificazioni ed integrazioni alle norme del codice penale e di procedura penale in tema di criminalità informatica*", introduce nel nostro ordinamento 14 nuove norme penali, disposte tutte nel libro II[54]. Citandone alcune, ricordiamo: accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* C.P.), detenzione e diffusione abusiva dei codici di accesso a sistemi informatici (art. 615-*quater* C.P.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* C.P.), installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* C.P.).
Durante il processo di elaborazione di norme dirette a sanzionare le forme di abuso della tecnologia informatica, il legislatore ha dovuto operare un bilanciamento fra due esigenze opposte, quali la necessità di ricorrere a termini tecnici per descrivere precisamente e sinteticamente il fenomeno sottostante, e il bisogno di utilizzare termini che fossero il più possibile "sganciati" dalla tecnologia, questo a causa della volontà di contrastare la rapida obsolescenza delle norme a causa dei prossimi sviluppi della tecnologia[55].
I *cybercrimes* si evolvono molto rapidamente a causa delle continue e ormai inarrestabili innovazioni tecnologiche, e il nostro legislatore fa il possibile per fronteggiare le nuove minacce e adeguarsi ai cambiamenti.

---

[52] Amore, S. 2006. *Internet ed il diritto penale. I crimini informatici: dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Halley Editrice.
[53] Del Re, C. 2009. *Formazione di un nuovo fenomeno criminale: i reati informatici. La frode informatica*, Edizioni Polistampa, Firenze.
[54] Del Re, C. 2009. *Formazione di un nuovo fenomeno criminale: i reati informatici. La frode informatica*, Edizioni Polistampa, Firenze.
[55] Del Re, C. 2009. *Formazione di un nuovo fenomeno criminale: i reati informatici. La frode informatica*, Edizioni Polistampa, Firenze.

È constatato che l'informatica avanzi assai più rapidamente rispetto a quanto possano fare le leggi ed è per questo motivo che, nonostante la normativa italiana sui cybercrimes sia una delle più recenti, ci si trova spesso davanti a vuoti normativi a cui difficilmente si è in grado di porre rimedio.

2. *La Convenzione di Budapest*

Uno degli obiettivi comune a tutti gli Stati membri è quello di combattere il crimine informatico in maniera coordinata: ai fini del perseguimento di questo obiettivo, il 23 novembre 2001 è stato firmato nell'ambito del Consiglio d'Europa il primo accordo internazionale che riguarda i crimini realizzati per mezzo di internet o altre reti informatiche. Ratificata nell'ordinamento italiano con la Legge 18 marzo 2008, n.48, la Convenzione di Budapest si impone di armonizzare i sistemi penali nazionali e le relative disposizioni connesse nell'ambito della criminalità informatica, prevedendo a tal fine gli strumenti necessari per l'indagine e il perseguimento di questi reati, inclusa la cooperazione internazionale.

È considerata il primo strumento giuridico internazionale nel campo del cybercrime: ha per la prima volta introdotto nozioni di tipo tecnico in materia digitale, fornendo così una definizione ai termini più usati nel linguaggio del web con particolare riferimento ai crimini informatici[56].

La Convenzione si fonda sulla consapevolezza che le nuove tecnologie mettono a tutti gli effetti in discussione i concetti legali esistenti: le leggi nazionali, limitate tradizionalmente ad uno specifico territorio, non sono sufficienti a fronteggiare il problema della localizzazione del luogo in cui agiscono i criminali informatici, luogo diverso da quello in cui gli atti producono i loro effetti. Gli Stati si sono infatti consapevolizzati del fatto che le possibili soluzioni a queste problematiche vanno rintracciate nel diritto internazionale, sempre rispettando i diritti umani[57].

---

[56] Santarelli, M. 2023. *Lotta al cyber crimine, ecco il secondo protocollo addizionale alla convenzione di Budapest: le finalità*, in *Network Digital 360*, 21 febbraio, in https://www.cybersecurity360.it/cybersecurity-nazionale/lotta-al-cyber-crimine-ecco-il-secondo-protocollo-addizionale-alla-convenzione-di-budapest-le-finalita/.

[57] Mattarella, A. 2022. *La futura Convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, in *Sistema Penale*, Fascicolo 3, pp. 60-102.

Tutti gli obiettivi che si pone di raggiungere la Convenzione possono essere riassunti in "armonizzazione normativa" e "cooperazione internazionale"[58]. Dal punto di vista sostanziale[59], sono state introdotte dalla Convenzione le fattispecie di accesso illecito, interferenza di dati, uso improprio di dispositivi, intercettazione illecita, interferenza in un sistema, frode informatica, reati in materia di diritto d'autore e pedopornografia.

La Sezione 1 (artt. 2-13) ha lo scopo di prevenire e reprimere la criminalità informatica fissando uno standard minimo comune per le fattispecie di reato incluse nell'elenco (reati informatici, reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici), che può eventualmente essere esteso dal diritto interno di ogni singolo Stato; il Capo II tratta le disposizioni in merito alla giurisdizione, il Capo III tratta la materia dell'assistenza giudiziaria e della criminalità informatica, oltre alle norme in materia di estradizione. La Convenzione prevede inoltre che in mancanza di una disciplina giuridica specifica, un trattato oppure una specifica convenzione, si applicano le disposizioni contenute nella Convenzione, invece dove nell'ordinamento nazionale esiste una normativa, le disposizioni esistenti si applicano anche all'assistenza[60].

Agli inizi vi è stata una certa diffidenza nei confronti della Convenzione, che si è poi trasformata in largo consenso, fintanto che nel 2006 si è giunti all'approvazione da parte del Consiglio Europeo di un primo protocollo addizionale: il "Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici"[61].

Di recente è stato autorizzato dal Consiglio Europeo anche il secondo protocollo addizionale alla convenzione di Budapest, il "Second Additional Protocol to che Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence": datato 12 maggio 2022, questo documento va ad integrare il quadro interno

---

[58] Santarelli, M. 2023. *Lotta al cyber crimine, ecco il secondo protocollo addizionale alla convenzione di Budapest: le finalità*, in *Network Digital 360*, 21 febbraio, in https://www.cybersecurity360.it/cybersecurity-nazionale/lotta-al-cyber-crimine-ecco-il-secondo-protocollo-addizionale-alla-convenzione-di-budapest-le-finalita/.

[59] Picotti, L. 2008. *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, Fascicolo 5, pp. 437-448.

[60] Mattarella, A. 2022. *La futura Convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, in *Sistema Penale*, Fascicolo 3, pp. 60-102.

[61] Santarelli, M. 2023. *Lotta al cyber crimine, ecco il secondo protocollo addizionale alla convenzione di Budapest: le finalità*, in *Network Digital 360*, 21 febbraio, in https://www.cybersecurity360.it/cybersecurity-nazionale/lotta-al-cyber-crimine-ecco-il-secondo-protocollo-addizionale-alla-convenzione-di-budapest-le-finalita/.

dell'UE riguardante l'accesso alle prove elettroniche. Fra i principali scopi vi sono quello di favorire l'accesso transfrontaliero alle prove elettroniche che possono essere utilizzate durante i procedimenti penali, inoltre si pone l'obiettivo di facilitare la collaborazione fra gli Stati membri nella lotta al cyber crime garantendo il rispetto della normativa dell'UE nell'ambito della protezione dei dati. In questo protocollo sono state anche stabilite le procedure per l'assistenza giudiziaria reciproca d'urgenza[62].

La Convenzione di Budapest ha raffigurato una prima base per una implementazione del contrasto al fenomeno dei crimini informatici: tuttavia, è stata ratificata da solo 68[63] Stati.

Uno strumento che vanta scarsa adesione non può rappresentare una futura guida solida nella lotta alle nuove forme di criminalità, proprio per questo dobbiamo fare riferimento anche al ruolo "suppletivo" svolto dalla Convenzione Onu contro il crimine organizzato transnazionale, sottoscritta a Palermo nel 2000. Quest'ultima, che vede la partecipazione di oltre 190 Stati, è il principale strumento internazionale di riferimento contro tutte le possibili forme di criminalità, prevedendo norme innovative nell'ambito delle indagini, della sorveglianza elettronica, della cooperazione giudiziaria e della responsabilità da reati degli enti.

Fornisce una nozione ampia di "reato grave" di dimensione transnazionale e di "gruppo criminale organizzato": quest'ultimo viene definito come "un gruppo strutturato, esistente per un periodo di tempo, composto da tre o più persone che agiscono di concerto al fine di commettere uno o più reati gravi o reati stabiliti dalla presente Convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale". Questa definizione è stata elaborata al fine di renderla suscettibile di essere recepita dai singoli Stati nazionali e che si mostrasse idonea a rappresentare il fenomeno del crimine organizzato transnazionale[64].

---

[62] Santarelli, M. 2023. *Lotta al cyber crimine, ecco il secondo protocollo addizionale alla convenzione di Budapest: le finalità*, in *Network Digital 360*, 21 febbraio, in https://www.cybersecurity360.it/cybersecurity-nazionale/lotta-al-cyber-crimine-ecco-il-secondo-protocollo-addizionale-alla-convenzione-di-budapest-le-finalita/.

[63] Berti, R., Zumerle F. 2023. *Convenzione ONU sul cybercrime in dirittura d'arrivo: perché è importante, i problemi*, in *Network Digital 360*, 19 aprile, in https://www.agendadigitale.eu/sicurezza/convenzione-onu-sul-cybercrime-in-dirittura-darrivo-perche-e-importante-i-problemi/.

[64] Mattarella, A. 2022. *La futura Convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, in *Sistema Penale*, Fascicolo 3, pp. 60-102.

È opportuno ricordare che l'Italia è stato uno fra i primi Paesi europei a provvedere all'introduzione di una legge organica in tema dei crimini informatici, la Legge 23 dicembre 1993, n.547. Prendendo in considerazione questo fatto, pur essendo nel nostro Paese già in vigore una disciplina potenzialmente esaustiva, considerata in certi casi "più incisiva[65]" di quella richiesta dalle disposizioni della Convenzione di Budapest, si è ritenuto comunque opportuno, ai fini di una migliore collocazione sistematica, procedere con l'integrazione e la modifica di certe disposizioni del nostro codice penale: per questo è stato presentato il 19 giugno 2007 alla Camera dei Deputati il disegno di legge con oggetto la ratifica proprio della Convenzione di Budapest.

Soffermandoci sulla posizione che ha preso la Convenzione di fronte al fenomeno dei *cybercrime*, si nota che la Convenzione tende a trattare il cybercrime come un semplice reato, cioè come un problema interno che necessita di essere gestito in modo unilaterale dal paese offeso: tutt'oggi è indubbio che il cybercrime sia una forma di reato, ma può essere definito come un qualcosa di più di un normale reato, infatti questo non è basato territorialmente; una delle principali differenze rispetto ai reati è che il cybercrime è in grado di trascendere facilmente i confini nazionali, e la Convenzione come risposta a questa circostanza ha deciso di rispondere richiedendo ai paesi di assistersi l'uno con l'altro attraverso investigazioni e persecuzioni nazionali[66].

In questo contesto è opportuno citare il Consiglio dell'Unione Europea, il quale nella "Decisione quadro relativa agli attacchi ai sistemi di informazione" afferma che: "qualora un reato rientri nella giurisdizione di più di uno Stato membro e quando ciascuno degli Stati interessati potrebbe validamente avviare un'azione penale sulla base degli stessi fatti, gli Stati membri interessati cooperano per decidere quale di essi perseguirà gli autori del reato allo scopo, se possibile, di concentrare i procedimenti in un solo Stato membro. A tal fine, gli Stati membri possono fare ricorso a qualsiasi organismo o meccanismo istituito all'interno dell'Unione europea per agevolare la cooperazione tra le loro autorità giudiziarie ed il coordinamento del loro operato"[67].

---

[65] Del Re, C. 2009. *Formazione di un nuovo fenomeno criminale: i reati informatici. La frode informatica*, Edizioni Polistampa, Firenze.

[66] Del Re, C. 2009. *Formazione di un nuovo fenomeno criminale: i reati informatici. La frode informatica*, Edizioni Polistampa, Firenze.

[67] Amore, S. 2006. *Internet ed il diritto penale. I crimini informatici: dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Halley Editrice.

3. *La politica dell'UE in materia di cybersicurezza*

Una delle priorità principali dell'UE è quella di promuovere la digitalizzazione, rafforzando la sua sovranità digitale stabilendo standard propri, piuttosto che perseguire quelli stabiliti da altri: per guidare la trasformazione digitale, è stato presentato un programma politico che contiene traguardi e obiettivi che l'UE si propone di raggiungere per il 2030, in settori che spaziano dalle infrastrutture digitali sicure e sostenibili, alla digitalizzazione dei servizi pubblici fino alla regolamentazione dell'intelligenza artificiale[68].

Con la diffusone della digitalizzazione, è diventato un aspetto fondamentale quello della protezione dalle minacce informatiche, al fine di mantenere un buon funzionamento della società. I cyberattacchi sono sempre più frequenti: la Commissione europea ha stimato che i costi del cybercrime per l'economia globale abbiano raggiunto i 5,5 trilioni entro la fine del 2020[69]. I cyber attacchi in certi contesti sono una potente arma di interruzione di massa, in grado di causare forti impatti in ambito economico e sociale, ed è anche per questo motivo che il legislatore europeo si è spinto verso la ricerca di adeguate risposte innovative e coordinate da parte di tutti gli Stati membri per assicurare la continuità dei servizi digitali nel caso in cui subentrino incidenti di sicurezza.

Dopo una revisione della Direttiva NIS (Network and Information Security), Direttiva UE 2016/1148 del 6 luglio 2016 sulla sicurezza delle reti e delle informazioni (attuata in Italia con d.lgs. n. 65 del 18 maggio 2018), e avendo constatato alcune carenze intrinseche che hanno ostacolato l'affronto di sfide attuali in materia di sicurezza informatica, si è giunti all'elaborazione della Direttiva NIS 2, nell'ottica di raggiungere una piena definizione della strategia per la cybersicurezza dell'UE.

---

[68] Parlamento europeo, 2021. *Plasmare la trasformazione digitale: spiegazione della strategia dell'UE*, 22 aprile, in https://www.europarl.europa.eu/news/it/headlines/society/20210414STO02010/plasmare-la-trasformazione-digitale-spiegazione-della-strategia-dell-ue.

[69] Parlamento europeo, 2022. *Criminalità informatica: le nuove misure dell'UE per rafforzare la cibersicurezza*, 10 novembre, in https://www.europarl.europa.eu/news/it/headlines/security/20221103STO48002/criminalita-informatica-nuove-misure-dell-ue-per-rafforzare-la-cibersicurezza?at_campaign=20234-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=DSA&at_goal=TR_G&at_audience=&at_topic=Cybersecurity&gclid=CjwKCAjw-vmkBhBMEiwAlrMeF9xdar5ODLQJzbfMz0V9Pzl0aK7lit53xNpryID6rt_RYzfU65REABoCKHQQAvD_BwE

La Direttiva NIS 2 fornisce agli Stati membri la possibilità di istituire una o più autorità nazionali competenti che siano responsabili della cyber sicurezza e che si occupino di supervisione. Altro passo importante compiuto da questa norma è l'istituzione della rete europea di organizzazioni di collegamento per le crisi informatiche: CyCLONe, ovvero Cyber Crisis Liaison Organisation Network, che ha il ruolo di supportare la gestione coordinata di incidenti, su larga scala, di sicurezza informatica[70].

Anche a livello europeo vi è un'agenzia responsabile della cyber sicurezza: stiamo parlando di ENISA, European Network and Information Security Agency, l'Agenzia dell'Unione europea per la sicurezza informatica, che fornisce sostegno agli Stati membri dell'UE, oltre che ai singoli cittadini, al fine di promuovere le migliori pratiche di sicurezza informatica, aumentare la comprensione di rischi e minacce informatiche e promuovere una maggior coordinazione tra gli Stati membri con riguardo ai temi di sicurezza informatica delle PMI. Tale agenzia collabora soprattutto con le organizzazioni e le imprese al fine di rafforzare la fiducia nell'economia digitale, inoltre contribuisce anche all'attuazione della sopracitata Direttiva NIS 2[71].

Istituita nel 2004[72], ENISA ha fornito un importante contributo anche in merito al problema della carenza di forza lavoro nel settore della cybersicurezza, che unito al divario di competenze risultano essere fra le principali preoccupazioni per la sicurezza nazionale in campo cyber. A fronte di ciò, ENISA ha individuato la necessità di adottare un piano comune per la definizione di ruoli e competenze in materia di cybersicurezza, che possa essere sfruttato per risolvere i problemi citati: è così che nasce ECSF, acronimo di European Cybersecurity Skills Framework, ovvero il quadro europeo delle competenze in materia della cybersicurezza, avente lo scopo di rafforzare la cultura europea della cybersecurity, realizzando così un importante passo in avanti verso un'Europa sempre più digitale. Tale ECSF è uno strumento pratico per agevolare e

---

[70] Spagnoli, C. 2023. *Direttiva NIS 2: la sicurezza delle infrastrutture critiche, tra normativa e buone prassi*, in *Network Digital 360*, 5 aprile, in https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-la-sicurezza-delle-infrastrutture-critiche-tra-normativa-e-buone-prassi/.

[71] Boccellato, P. 2023. *PMI e cybersecurity, ENISA rilascia un tool per 'testare' la sicurezza delle piccole e medie imprese*, in *Cybersecurity Italia*, 4 aprile, in https://www.cybersecitalia.it/pmi-e-cybersecurity-enisa-rilascia-un-tool-per-testare-la-sicurezza-delle-piccole-e-medie-imprese/24041/.

[72] Tosoni, L. 2019. *Cybersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT*, in *Network Digital 360*, 7 giugno, in https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/.

supportare l'identificazione di compiti, abilità e competenze oltre alle conoscenze, abbinate ai ruoli dei professionisti europei nel campo della cybersecurity[73].

Dal momento in cui le istituzioni europee hanno approvato la Direttiva NIS nel 2016, stanno continuando ad adottare misure che siano volte al rafforzamento della sicurezza cibernetica nell'UE, affiancandosi quindi alla Direttiva NIS. Di recente è stata adottata una misura consistente in un Regolamento volto alla creazione di un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali, inoltre si pone anche il compito di rafforzare il ruolo di ENISA: tale Regolamento prende il nome di Cybersecurity Act, ed è stato pubblicato in Gazzetta Ufficiale il 7 giugno 2019, entrato poi in vigore il successivo 27 giugno 2019.

Lo strumento normativo in questione risulta essere una parte indispensabile nella nuova strategia dell'UE per la sicurezza cibernetica: mira alla creazione di un mercato unico della sicurezza cibernetica in quanto ai prodotti, servizi e processi, e si pone come obiettivo anche quello di aumentare la fiducia da parte dei consumatori nei confronti delle tecnologie digitali. Si tratta di un Regolamento, perciò una volta entrato in vigore non vi è necessità di interventi attuativi da parte dei singoli legislatori nazionali ma sarà immediatamente applicabile in tutti gli Stati membri.

Il Cybersecurity Act si è occupato di rafforzare il ruolo dell'ENISA, garantendo a questa un mandato permanente e consentendole di svolgere, oltre ai compiti di consulenza tecnica già di sua competenza, anche attività di supporto alla gestione degli incidenti informatici, facendo si che possa fornire un sostegno più concreto agli Stati membri[74].

Parlando delle questioni che l'UE si è trovata a dover affrontare, negli ultimi anni a fronte delle questioni sorte in merito al tema della responsabilità dei gestori dei servizi in rete, è stato definitivamente affermato dalla Commissione europea che l'unica forma di responsabilità che può essere delineata a carico di tali soggetti è una forma di responsabilità *ex post*, fondata principalmente sulla mancata rimozione dei contenuti illeciti di cui gli intermediari siano a conoscenza, raffigurabile in un dovere di diligenza

---

[73] Di Franco, F. 2022. *ENISA: "Nasce il quadro europeo delle competenze di cybersecurity, ecco perché è importante"*, in *Network Digital 360*, 9 dicembre, in https://www.agendadigitale.eu/sicurezza/cybersicurezza-arriva-il-quadro-europeo-delle-competenze-ecco-perche-e-importante/.

[74] Tosoni, L. 2019. *Cybersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT*, in *Network Digital 360*, 7 giugno, in https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/.

in capo ai gestori dei servizi in rete. Con riguardo a tale problema, sono state individuate quattro aree di intervento, le quali sono state seguite da proposte di provvedimenti normativi: queste riguardano la proliferazione di piattaforme di condivisione di video online con contenuti nocivi per i soggetti deboli quali i minori, e istigazione all'odio; l'utilizzo online di contenuti protetti dal diritto d'autore, la lotta contro gli abusi sessuali sui minori e la pedopornografia online, e infine l'area di intervento concernente la lotta al cyber-terrorismo.

Dunque, le istituzioni europee hanno scelto di adottare un approccio di tipo settoriale, ma emerge comunque una linea che accomuna gli interventi nell'ambito della gestione delle piattaforme online a livello europeo: si concentra l'attenzione sulla necessità di prevedere interventi volti alla rimozione da parte degli intermediari dei contenuti che risultano lesivi di interessi e posizioni giuridicamente rilevanti, con un'incisività delle misure diversa a seconda della gravità del contenuto illecito.

Da questa riflessione emerge che a livello europeo vi è l'esigenza di una maggiore responsabilizzazione di coloro che prestano servizi in rete, considerando il ruolo fondamentale che questi possono svolgere al fine di contrastare i fenomeni criminosi che avvengono nel cyberspazio: questa esigenza potrà essere soddisfatta da future norme europee e dalla loro necessaria attuazione[75].

4. *L'Agenzia Nazionale per la cybersicurezza (ACN)*

L'Agenzia, istituita con il decreto-legge 14 giugno 2021, n. 82[76], ed operativa dal 1° settembre 2021, è stata creata appositamente per gestire la cyber security nazionale in Italia, ed è posta sotto il controllo diretto del COPASIR (Comitato parlamentare per la sicurezza della Repubblica); è istituita in capo alla Presidenza del Consiglio dei Ministri.

All'interno dell'Agenzia è inoltre incluso il Nucleo per la Sicurezza Cibernetica (NSC), che, prima della creazione dell'ACN, era sotto il controllo del DIS (Dipartimento delle

[75] Panattoni, B. 2019. *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online*, in *Diritto Penale Contemporaneo - Rivista Trimestrale*, Vol. 2, pp. 35-52.

[76] Fusco, E. 2023. *Riflessioni e proposte in tema di reati cyber*, in *Sistema Penale*, 28 aprile, in https://www.sistemapenale.it/it/opinioni/fusco-riflessioni-e-proposte-in-tema-di-reati-cyber.

Informazioni per la Sicurezza); questa inclusione deriva dalla volontà di far si che il DIS si concentri solo sul suo compito principale, che è coordinare l'AISE (Agenzia Informazioni e Sicurezza Esterna) e l'AISI (Agenzia Informazioni e Sicurezza Interna), le due agenzie di intelligence[77].

Fra le principali funzioni dell'Agenzia vi sono: l'esercizio delle funzioni di Autorità nazionale in materia di cybersecurity ai fini di tutela degli interessi nazionali da eventuali minacce cibernetiche; lo sviluppo di capacità nazionali di prevenzione, monitoraggio, rilevamento e mitigazione per fronteggiare gli incidenti di sicurezza informatica e gli attacchi informatici; contribuire ad innalzare la sicurezza dei sistemi di ICT dei soggetti presenti nel perimetro di sicurezza nazionale cibernetica, fra cui le Pubbliche Amministrazioni, gli operatori di servizi essenziali e i fornitori di servizi digitali; stimolare la crescita di una forza di lavoro nazionale nel campo della cybersecurity nell'ottica di autonomia nazionale strategica nel settore; coordinare soggetti pubblici per la realizzazione di azioni comuni in materia di cybersicurezza a livello nazionale, assumere il ruolo di interlocutore unico nazionale per soggetti sia pubblici che privati in materia di misure di sicurezza e attività ispettive nell'ambito della sicurezza nazionale cibernetica. Oltre a ciò, è autorità nazionale di certificazioni di cybersicurezza (ai sensi dell'art. 58 del regolamento UE 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019) e deve predisporre la strategia nazionale di cybersicurezza[78]. È inoltre competente per l'accertamento delle violazioni e l'irrogazione di sanzioni amministrative previste dal decreto legislativo NIS, ovvero il Decreto che stabilisce i requisiti minimi per la sicurezza delle reti e dei sistemi informativi dell'UE.

L'ACN e la Polizia di Stato hanno siglato un accordo di collaborazione ai fini della prevenzione e della gestione degli eventi cibernetici, collaborazione che già in passato si è mostrata efficace sia per quanto riguarda l'attuazione della strategia nazionale di cybersicurezza, sia in riferimento al livello operativo durante eventi significativi di sicurezza del Paese. Tale accordo prevede che l'ACN possa servirsi dei COSC (Centri

---

[77] Longo, A., Tarsitano, P. 2021. *Ecco l'Agenzia per la cybersicurezza nazionale: come cambia la sicurezza cibernetica dell'Italia*, in *Network Digital 360*, 8 agosto, in https://www.cybersecurity360.it/cybersecurity-nazionale/ecco-lagenzia-per-la-cybersicurezza-nazionale-come-cambia-la-sicurezza-cibernetica-dellitalia/.

[78] Longo, A., Tarsitano, P. 2021. *Ecco l'Agenzia per la cybersicurezza nazionale: come cambia la sicurezza cibernetica dell'Italia*, in *Network Digital 360*, 8 agosto, in https://www.cybersecurity360.it/cybersecurity-nazionale/ecco-lagenzia-per-la-cybersicurezza-nazionale-come-cambia-la-sicurezza-cibernetica-dellitalia/.

Operativi per la Sicurezza Cibernetica) della Polizia postale ai fini di attivare collaborazioni operative anche tramite l'individuazione di determinate professionalità della Polizia di Stato, le quali potranno vedersi impiegate presso l'Agenzia[79].

5. *Questioni giuridiche rilevanti: il locus commissi delicti*

Aspetti come la de-territorializzazione e la de-temporalizzazione che caratterizzano i reati informatici, facilitano la commissione di questi ultimi, rendendo possibile la loro realizzazione da qualsiasi parte del mondo e senza il bisogno di un collegamento fisico tra il sistema e l'utente.

Una problematica che risulta essere comune a tutti i reati commessi per mezzo di Internet è l'esatta individuazione del *locus commissi delicti*, ovvero del luogo in cui si sia realizzata la condotta o dove si sia verificato l'evento criminoso: la difficoltà emerge principalmente sia dalla natura transfrontaliera di questi reati, sia dalla scarsa omogeneità delle legislazioni penali, che provoca qualificazioni diverse della medesima condotta a seconda di quale ordinamento giuridico si considera[80].

Con l'introduzione della disciplina sui reati informatici è sorta poi anche la questione in merito all'individuazione del giudice competente territorialmente: il criterio individuato all'art. 8 comma 1 c.p.p., assumendo come regola generale il luogo nel quale il reato si è consumato, risultava impossibile applicarlo ai cybercrimes, data l'impossibilità di risalire al luogo in cui il fatto è avvenuto[81]. Inoltre, la difficoltà di adattare i concetti di delocalizzazione e de-temporalizzazione ha provocato la nascita di un'ulteriore problematica riguardante le definizioni dei concetti di stampa, domicilio e corrispondenza: la questione del concetto di stampa è stata risolta dalla Corte di Cassazione che ha optato per un'interpretazione estensiva del termine, prevedendo che occorre solamente il requisito della pubblicazione, indifferentemente dal supporto sul quale quest'ultima avviene; in merito al domicilio si è invece operata una equiparazione

[79] Ufficio stampa Polizia di Stato, 2023. *Siglato accordo tra Polizia e l'Agenzia per la cybersicurezza nazionale*, 26 aprile, in https://www.poliziadistato.it/articolo/siglato-accordo-tra-polizia-e-lagenzia-per-la-cybersicurezza-nazionale

[80] Amore, S. 2006. *Internet ed il diritto penale. I crimini informatici: dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Halley Editrice.

[81] Ruffilli, C. 2020. *I reati informatici e l'evoluzione del concetto di materialità*, in *Penale*, 15 luglio, in http://www.salvisjuribus.it/i-reati-informatici-e-levoluzione-del-concetto-di-materialita/.

del sistema informatico-telematico al domicilio, estendendo così la tutela prevista per la sfera individuale anche allo spazio virtuale; con riferimento alla corrispondenza, la legge n. 547/1993 ha introdotto il concetto di corrispondenza telematica, rendendo così applicabile anche al caso di posta elettronica la normativa in materia di violazione, sottrazione e soppressione di corrispondenza, con la particolarità che a differenza della corrispondenza cartacea, di norma accessibile unicamente dal destinatario, nella corrispondenza telematica è necessaria una legittimazione che abiliti alla conoscenza delle informazioni in esso custodite, perciò nel caso in cui il sistema fosse protetto da password, si ritiene che la corrispondenza sia disponibile lecitamente da parte di coloro che dispongono della chiave informatica di accesso, legittimamente[82].

Il legislatore ha quindi introdotto nuove norme che siano in grado di garantire una efficace risposta a quelle che sono le nuove forme di aggressione rese possibili dall'evoluzione tecnologica. Tuttavia, nonostante le buone intenzioni del legislatore, vi sono delle ipotesi di reato che risultano essere più problematiche di altre: stiamo parlando dell'accesso abusivo ad un sistema informatico o telematico, per il quale tutt'oggi non si è giunti ad un orientamento univoco.

Con riguardo al primo, ovvero l'accesso abusivo ad un sistema informatico o telematico disciplinato all'articolo 615 *ter* c.p., l'individuazione del locus commissi delicti è problematica e vi sono tre diversi orientamenti che cercano di dare una soluzione a questo problema: un primo orientamento si convince del fatto che il luogo di consumazione corrisponda al luogo in cui si trova il server violato[83]; in un secondo orientamento vede assumere rilevanza "il luogo di ubicazione della postazione con cui l'utente accede o si introduce nel sistema che contiene l'archivio informatico"[84]; un terzo orientamento preferisce invece la tesi che prevede l'individuazione del locus commissi delicti facendo riferimento al comportamento del soggetto agente, invece che il luogo in cui è materialmente collocato il *server* che controlla le credenziali con cui il *client* accede[85]. La questione rimane tuttavia aperta.

---

[82] Ruffilli, C. 2020. *I reati informatici e l'evoluzione del concetto di materialità*, in *Penale*, 15 luglio, in http://www.salvisjuribus.it/i-reati-informatici-e-levoluzione-del-concetto-di-materialita/.

[83] Cass. Pen., 27 settembre 2013, Sez. I, sent. n. 40303.

[84] Cass. Pen., 26 marzo 2015, Sez. Un., sent. n. 17325.

[85] Facciolini, T. 2022. *I reati commessi su internet: individuazione del locus commissi delicti*, in *Penale*, 31 gennaio, in http://www.salvisjuribus.it/i-reati-commessi-su-internet-individuazione-del-locus-commissi-delicti/.

La legge 23 dicembre 1993, n. 547 ha introdotto apposite norme riguardanti l'inviolabilità del domicilio: l'istituto del domicilio fino a qualche anno fa era inteso come un luogo fisico e tangibile, visibile dove il soggetto abbia stabilito la sede principale dei suoi affari e interessi. Il concetto di domicilio, inteso tradizionalmente come luogo fisico in cui chiunque può accedervi, se associato al concetto di digitale e quindi assumendo le sembianze di un luogo astratto, fa sorgere forti dubbiosità sul funzionamento della tutela penale[86].

Il domicilio informatico può essere definito come quello "spazio ideale di pertinenza della persona (fisica o giuridica), oggetto di tutela della propria riservatezza in maniera assolutamente analoga rispetto alla riservatezza individuale"[87]: il domicilio informatico deve essere protetto non sono al fine di impedire la violazione della riservatezza della vita privata, ma anche qualsiasi tipologia di intrusione[88].

La volontà del legislatore di equiparare il concetto di domicilio "fisico" a quello di domicilio digitale si ritrova nell'art. 615-*ter* c.p., che punisce "*chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*". Questa previsione legislativa italiana non sembra però essere immune da alcune perplessità rispetto al principio di lesività: di fatto in questo contesto potrebbe dirsi anticipata, constatando la mancanza di qualunque riferimento rispetto alla presa di conoscenza dei dati contenuti nel sistema su cui il soggetto agente compie la violazione[89].

Fra i reati informatici definiti impropri, cioè i reati comuni che eventualmente possono essere commessi con il supporto di tecnologie informatiche, troviamo la "diffamazione *online*", cioè l'offesa dell'altrui decoro che avviene sul web. Relativamente all'individuazione del *locus commissi delicti* in tema di diffamazione online, non vi è

---

[86] Di Santo, A. 2022. *La protezione del domicilio informatico sul piano penale: un'intrinseca contraddizione?*, in *Penale*, 12 maggio, in https://www.altalex.com/documents/news/2022/05/12/protezione-domicilio-informatico-piano-penale-intrinseca-contraddizione.

[87] D'Aiuto, G., Levita, L. 2012. *I reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè.

[88] Di Prisco, A. 2020. *Cybersecurity e reati informatici: due ipotesi a confronto*, in *Ius in itinere*, 27 gennaio, in https://www.iusinitinere.it/cybersecurity-e-reati-informatici-due-ipotesi-a-confronto-25224.

[89] Di Santo, A. 2022. *La protezione del domicilio informatico sul piano penale: un'intrinseca contraddizione?*, in *Penale*, 12 maggio, in https://www.altalex.com/documents/news/2022/05/12/protezione-domicilio-informatico-piano-penale-intrinseca-contraddizione.

una visione uniforme della questione da parte di dottrina e giurisprudenza: la giurisprudenza con due sentenze del 2011 ha affermato che ai fini dell'individuazione della competenza non è possibile utilizzare criteri univoci come la prima pubblicazione, l'immissione della notizia in rete o l'accesso del primo visitatore, nemmeno il criterio del luogo in cui è localizzato il server in cui il provider alloca la notizia. La Suprema Corte è giunta alla conclusione che in questo particolare contesto sia necessario fare ricorso al criterio del luogo di domicilio dell'imputato, in quanto il server può trovarsi ovunque e i dati inseriti non partono dal server verso alcuna destinazione, ma bensì restano immagazzinati a disposizione dei singoli utenti che leggono dal proprio terminale, quindi anche nel caso in cui esista uno specifico luogo di partenza delle informazioni, questo non coincide comunque con quello di verificazione dell'evento lesivo, da individuare nel luogo in cui si attiva il collegamento. La Corte conclude affermando che il *locus commissi delicti* della diffamazione telematica è da individuare nel luogo in cui le offese e denigrazioni vengono percepite da più soggetti che fruiscono della rete, e quindi nel luogo in cui viene attivato il collegamento, questo anche nel caso in cui il sito web sia registrato all'estero, sempre però che l'offesa sia stata percepita da più soggetti che si trovano in Italia durante la fruizione. Utilizzando invece il criterio della residenza dell'imputato, si verifica un'eccessiva sottovalutazione della dimensione dell'evento, e la persona offesa si troverebbe costretta a far valere le sue ragioni in luoghi assai distanti rispetto a quello in cui si è verificata una lesione alla sua reputazione.

Sono state sollevate nel corso del tempo varie questioni in merito alla configurazione del luogo in cui viene commesso tale reato: come soluzione risulta auspicabile, per un'ottica di certezza del diritto, un'opzione elaborata dalle Sezioni Unite civili della Cassazione che con una pronuncia hanno affermato che l'evento si verifica quando e dove si configura nell'immediato come danno risarcibile, e tale luogo sembra essere quello in cui si estrinseca la vita di relazione del danneggiato, il che consente alla persona offesa di far valere le proprie ragioni nel luogo in cui è stata colpita dalla condotta diffamatoria[90].

[90] Zunica, F. 2023. *Il diritto penale del web tra sforzi ermeneutici e nuove prospettive*, in *Diritto, Giustizia e Costituzione*, 12 maggio, in https://www.dirittogiustiziaecostituzione.it/il-diritto-penale-del-web-tra-sforzi-ermeneutici-e-nuove-prospettive-seconda-parte-di-fabio-zunica/.

Alla fine di questa breve esposizione delle principali questioni giuridiche che nel corso degli anni hanno interessato maggiormente i reati informatici e la loro regolamentazione, possiamo affermare che il diritto penale del web si trova ancora in difficoltà nel conciliare le tradizionali categorie di reati e queste nuove tipologie, i cybercrimes, e nel trovare un equilibrio fra le sfide che la contemporaneità digitale propone e i meccanismi di garanzia che troviamo nei principi del diritto penale.

CAPITOLO 3 - LA GOVERNABILITÀ DEL CYBERSPAZIO

1. *Lex informatica: il code diventa legge*

Fattori quali la globalizzazione, lo sviluppo di nuove tecnologie e la diffusione di reti globali hanno contribuito al verificarsi di un continuo mutamento della tradizionale configurazione delle tipologie di fonti del diritto, provocando così problemi di giurisdizione e dando vita a nuovi diritti, con la conseguenza che quelli già riconosciuti hanno inevitabilmente subito modifiche, in quello che è il loro originario significato, non indifferenti[91].

Maestri intende riferirsi con il termine *Lex informatica* a quell'insieme di regole che sono imposte dalla tecnologia per le reti di comunicazione e i flussi informatici[92]: questa legge informatica diventa a tutti gli effetti un sistema di regole parallelo, concorrente, e in certi casi addirittura sovrastante rispetto alle norme giuridiche.

Fra le principali differenze vi è il fatto che nel caso della regolazione giuridica il quadro normativo risulta essere rappresentato dalla legge, mentre invece nel caso della *Lex informatica* ci ritroviamo a poter definire il rispettivo quadro normativo come un insieme di architetture tecnologiche e standard predefiniti di rete.

In Internet, il diritto risulta veicolato tramite il codice: si utilizza il termine "*code"* per fare riferimento a quei codici sorgente, agli algoritmi, software, hardware, protocolli informatici e codice binario che vengono utilizzati dai programmatori informatici per strutturare ed architettare la rete, stabilendo così i vari modi d'uso delle tecnologie informatiche[93].

Maestri sostiene che a governare sia il codice, l'algoritmo binario, non la legge: software e hardware hanno un ruolo importante nel definire ciò che è eticamente lecito e i limiti del possibile tecnico, facendo diventare così lecito tutto ciò che è tecnicamente

---

[91] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[92] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[93] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

possibile. In questo modo entra in crisi la centralità che aveva il diritto, inteso come "fonte primaria del modo di comportarsi[94]".

Lawrence Lessing si è occupato di coniare l'espressione "*code is law*[95]" dimostrando come le architetture tecnologiche di Internet siano in possesso di loro codici e linguaggi normativi di auto-organizzazione che si occupano di stabilire e controllare le regole per l'accesso e per l'uso delle informazioni che troviamo in Rete: il codice sembra essere diventato non soltanto l'unica legge che regola il Cyberspazio, ma una vera e propria legge. Il *code* (codice) nella realtà dei fatti non è una legge, né è soggetto a limiti costituzionali: funziona però come una legge e possiede la copertura della legge.

Il fatto che il codice diventi legge non significa però che gli Stati siano impossibilitati nel poter regolare il Cyberspazio: viceversa, vuol dire che l'intervento sul codice e sull'architettura di sistema è l'unica capacità di regolamentazione che essi possiedono[96].

Fra gli strumenti di controllo atti a regolamentare le azioni degli utenti e a limitarne la libertà prodotti dal web vi sono le password di accesso, i *cookies*, la tracciabilità degli indirizzi IP, come anche l'autenticazione[97].

Il codice è una delle forme attraverso le quali si esprime il soft law, ovvero una serie di atti che, anche se privi di effetti giuridici vincolanti, risultano comunque giuridicamente rilevanti: è così che il *code* diventa legge.

È di fatto l'architettura del *code* che delinea le caratteristiche del dato trasmesso su Internet: la de-materializzazione e la de-territorializzazione (Maestri cita l'esempio dei beni intangibili come ad esempio i brani musicali in formato MP3[98]).

In una società in cui il *code* detta la legge, si smaterializzano quelle garanzie che avrebbero dovuto mettere in guardia le persone dal potere tecnologico. Il *code* è in grado di razionalizzare le procedure ma non può, a differenza di un giudice, considerare quegli accadimenti di difficile prevedibilità: ciò che bisogna avere ben chiaro è che la

---

[94] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

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

[96] Betzu, M. 2012. *Regolare Internet. Le libertà di informazione e di comunicazione nell'era digitale*, Giappichelli, Torino.

[97] Maestri, E. 2017. *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 15-26.

[98] Maestri, E. 2017. *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 15-26.

macchina non è in grado di sostituire completamente l'operato dell'uomo nel momento in cui si devono salvaguardare i diritti e punire le violazioni delle leggi.

La sociologa Saskia Sassen ha compiuto un'analisi su vari modelli di regolazione dello spazio digitale, e a suo avviso il dibattito sulla *governance* dell'Internet si divide sulla questione se questa possa essere o meno governata: alcuni sono sostenitori di una tesi che prevede che Internet possa essere un'entità soggetta ad un meccanismo di governo, mentre altri sostengono che sia una rete di reti decentrate e che si presti ad un coordinamento di norme e standard[99].

La dimensione in cui opera la *Lex informatica* si configura come una sorta di istituzione senza Stato entro la quale si vengono a dissolvere i particolarismi giuridici delle codificazioni nazionali e le differenze presenti fra i modelli di *common law* e *civil law*[100].

2. *Il dibattito fra cyberpaternalism e cyberlibertarianism*

Il concetto tradizionale di diritto che noi conosciamo ha subito negli anni, e sta continuando a subire notevoli trasformazioni: ad oggi risulta necessario ripensare le modalità con cui il diritto deve regolare le condotte che hanno luogo nel cyberspazio, e a ciò hanno provveduto due distinte visioni, quella del *cyberpaternalism* e quella del *cyberlibertarianism*[101].

Il dibattito sulla regolabilità o meno del cyberspazio, facendo riferimento ad un periodo che va dal 1996 al 2000, è stato dominato da due diverse scuole di pensiero: quella cyber-libertaria e quella cyber-paternalista. È stato il cyber-liberalismo a dominare le prime fasi dell'espansione di Internet, sostenendo la tesi che il cyberspazio fosse una società liberale autodeterminata e che la regolamentazione governativa doveva essere ridotta ai minimi livelli[102].

---

[99] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[100] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[101] Mingardo, L. 2020. *Il diritto delle macchine. Tecnodiritto e intelligenza artificiale in una prospettiva critica di informatica giuridica*, in *Anthropologica*, pp. 51-64.

[102] Wenguang, Y. 2018. *Internet Intermediaries' Liability for Online Illegal Hate Speech*, in *HeinOnline Law Journal Library*, Vol. 13, pp. 342-356.

I *cyber-libertarians* si sono da sempre rifiutati di riconoscere l'intervento dei governi nel cyberspazio, affermando che le caratteristiche intrinseche della progettazione di Internet rendevano qualsiasi manovra di intervento statale inutile.

Portavano avanti due visioni con riferimento alla regolamentazione del cyberspazio: una prima visione ottimistica, per la quale le tecnologie della libertà (termine utilizzato per riferirsi alla censura e al controllo, quindi a quegli strumenti e metodi per evitare la regolamentazione) saranno in grado di prendere il sopravvento sulla base del fatto che la tecnologia si sta evolvendo molto più rapidamente rispetto a quanto il governo possa adoperarsi tempestivamente per fronteggiarne l'evoluzione, adattandosi a nuovi metodi di regolazione. Mentre per quanto riguarda la visione pessimistica, i cyber-libertarians erano dell'idea che Internet sarebbe stato trasferito sotto il controllo dello Stato e, conseguentemente, si sarebbe verificato un annullamento della libertà online.

Ritenevano che non essendoci un singolo governo nello spazio reale (cioè nella dimensione in cui realmente ci troviamo) che fosse in grado di esercitare legittimamente il controllo su tutti i cittadini del cyberspazio e non essendoci la possibilità che i governi dello spazio reale prendano di mira solo i loro cittadini nel cyberspazio, constatando che la geografia del luogo non rientra nei confini fisici e che quindi a causa della natura senza confini dell'ambiente il governo non avesse la possibilità di controllare le azioni degli individui all'interno del cyberspazio, qualunque forma di intervento esterno da parte dei governi dello spazio reale sarebbe risultata illegittima.

La scuola cyber-libertaria sosteneva che, constatando che il cyberspazio "fluttuava al di sopra dello spazio reale[103]" non rispettando i confini dello spazio reale, le leggi approvate dagli Stati, in qualità di sovrani solo all'interno dei propri confini, sarebbero dovute fallire.

Consideravano Internet come uno strumento che favorisce l'arbitraggio normativo e che mina i tradizionali sistemi di controllo gerarchicamente strutturati: la legge del cyberspazio sarebbe determinata da una sorta di libero mercato di regolamenti nel quale gli utenti dell'Internet possono scegliere le regole che ritengono più consone.

In conclusione, per i *cyber-libertarians*, può essere efficace solo l'autoregolamentazione basata sulla volontà dei governati, poiché il diritto dell'ente normativo o dello Stato è

[103] Murray, A. 2011. *Nodes and Gravity in Virtual Space*, in *Legisprudence*, Vol. 5, pp. 195-221.

messo in discussione per colpa della mancanza di legittimità a governare oltre i confini[104].

Questa scuola di pensiero è stata fortemente criticata da coloro che si definiscono *cyber-paternalisti*, i quali ritengono che i *libertarians* basano le loro argomentazioni su una comprensione troppo semplificata dei fenomeni socio-politici: i *paternalisti* affermano che la concezione di libertà all'interno del cyberspazio sia in realtà un'illusione.

Inizialmente la questione era posta in merito alla regolamentazione o meno dell'Internet, ma con l'avvento del cyber-paternalismo ci si inizia a porre dei quesiti in merito al come e al chi debba governare questo spazio a-territoriale: i cyberpaternalisti hanno per la prima volta constatato che, con riferimento a Internet, quest'ultimo non sia non-regolabile in forza della sua architettura ma, al contrario, sia proprio regolato da questa.

Il cyberspazio non è libero ma è formato da una sfera altamente regolamentata e per i *cyber-paternalisti* questo è assai preoccupante, in quanto rappresenta uno spostamento di potere all'interno del Cyberspazio, permettendo così che azioni come ad esempio l'applicazione della legge sul diritto d'autore che nel mondo reale possono essere regolate solo dallo Stato, nel cyberspazio possano essere realizzate da privati tramite soluzioni basate su codici[105].

Il pensiero dei *cyber-paternalisti* nasce dal fatto che questi siano convinti che un cyberspazio non adeguatamente regolamentato sia indesiderabile[106], perché le attività dannose se non controllate portano al potenziale incremento di queste: i soggetti saranno portati a compiere condotte pericolose se sanno di non poter essere né controllati né sanzionati.

Il fatto che Internet sia accessibile a livello mondiale sta a significare che nessuna giurisdizione legale abbia il controllo *de jure* o *de facto* di tali attività: nessuna giurisdizione ha nessun controllo. Ma se consideriamo che Internet è accessibile da quasi tutto il mondo, le transazioni che nel mondo reale sarebbero state limitate ad un paio di giurisdizioni, nel caso del cyberspazio possono essere potenzialmente soggette a

[104] Murray, A. 2011. *Nodes and Gravity in Virtual Space*, in *Legisprudence*, Vol. 5, pp. 195-221.
[105] Murray, A. 2003. *The Regulatory Edge of the Internet*, in *International Journal of Law and Information Technology,* Vol 11, pp. 87-97.
[106] Murray, A. 2011. *Nodes and Gravity in Virtual Space*, in *Legisprudence*, Vol. 5, pp. 195-221.

tutte le giurisdizioni, facendo pensare che Internet, invece di essere un luogo virtuale non regolamentato, sia invece quello più pesantemente regolato al mondo[107].

Quindi di fatto, nella visione cyberpaternalistica, lo Stato rimane comunque quell'organismo che detiene il controllo dei rapporti che intercorrono, nel cyberspazio, fra i cittadini e le istituzioni[108].

I *cyberpaternalisti* hanno totalmente stravolto la visione della geografia del cyberspazio preferita dai *cyberlibertarians* come esaltazione della libertà e l'hanno trasformata in un luogo con molteplici giurisdizioni che si sovrappongono.

La libertà del cyberspazio sostenuta in precedenza dai cyberlibertarians è in realtà una pura illusione: lo spazio dell'Internet è altamente regolato, ed è proprio dall'architettura e dal codice che deriva questa regolazione.

3. *Il processo di de-territorializzazione*

Il principale problema delle norme giuridiche si individua nel fatto che la Rete si colloca, per sua natura, al di là del raggio di azione delle leggi statali, rendendo così difficile stabilire ad esempio come si possa perseguire chi ha agito in un certo Paese che è diverso da quello nel quale si è verificata la violazione della legge[109].

Irti[110] sostiene che in relazione all'evolversi delle tecnologie e alla necessità di strumenti di regolazione snelli e flessibili, non siano necessari dei nuovi strumenti di regolazione sul Web, ma che risulti invece sufficiente il ricorso ai tradizionali strumenti di formazione autoritativa, sostenendo quindi che, in relazione al problema della de-territorializzazione della Rete, tale quesito sia risolvibile mediante accordi interstatuali, affermando che "Si tratta di scegliere un luogo artificiale, deciso dalla volontà degli Stati, che permetta di individuare il diritto applicabile ed il giudice competente[111]".

Secondo l'opinione di Irti, la principale ragione dell'indebolimento della regolazione giuridica risiede nel fatto che il diritto è per sua essenza territoriale: si applica su un

---

[107] Murray, A. 2011. *Nodes and Gravity in Virtual Space*, in *Legisprudence*, Vol. 5, pp. 195-221.
[108] Mingardo, L. 2020. *Il diritto delle macchine. Tecnodiritto e intelligenza artificiale in una prospettiva critica di informatica giuridica*, in *Anthropologica*, pp. 51-64.
[109] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.
[110] Irti, N., Severino, E. 2001. *Dialogo su diritto e tecnica*, Laterza, Roma-Bari.
[111] Irti, N. 2006. *Norma e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari.

territorio che è ben definito e delimitato, mentre invece la tecnica è spaziale e transazionale, e in quanto de-territorializzata si presta meglio nella regolazione di una società globalizzata. All'indebolimento del diritto si è fornita una risposta con la nascita di un ordinamento giuridico sovranazionale in grado di creare uno spazio senza frontiere interne grazie al fatto che si va ad intrinsecare con quello nazionale[112].

La spazialità del diritto diviene la contro risposta alla spazialità della tecnica: si crea uno spazio che trascende i confini degli Stati, non un territorio. Cercando di creare spazi territoriali nuovi e più ampi, il diritto ha costruito un ambito spaziale de-territorializzato.

Pariotti[113] invece contribuisce a fornirci una visione più fiduciosa: sostiene infatti che se il diritto ha effettivamente natura territoriale, avrà sempre bisogno necessariamente di un "dove", e questo dove viene creato dalla globalizzazione tecnologica in un luogo ovunque. Questo "luogo terzo" consente la creazione di un diritto ovunque, globale, che permette di superare la concezione nazionalistica di questo.

Vari pensieri si pongono in contrasto con quello di Pariotti, come ad esempio quello di Severino[114], che afferma la superiorità della norma tecnica su quella giuridica e che la capacità della prima di travalicare il diritto nazionale fa si che nasca una vera e propria tecnocrazia, che prevede che tutto si realizzi solo attraverso norme tecniche; la tecnica diventa così la condizione universale per poter giungere alla realizzazione di qualunque scopo.

Suggestiva è la metafora coniata da Pietropaoli[115], con la quale egli paragona il Web alla rete dei pescatori: è un oceano caratterizzato da contorni indefiniti, e su questa superficie gli internauti, ovvero gli utenti del web, sono in grado di navigare, di fare *web-surfing*.

Così come il mare, il web evoca un non-luogo magico, mistico, un luogo di una vastità incontrollata che nasconde al suo interno una inimmaginabile quantità di risorse, di informazioni. Uno spazio definibile come potenzialmente pericolosissimo: terreno fertile per nuove opportunità criminali.

---

[112] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[113] Pariotti, E. 2004. *La giustizia oltre lo stato: forme e problemi*, Giappichelli, Torino.

[114] Irti, N., Severino, E. 2001. *Dialogo su diritto e tecnica*, Laterza, Roma-Bari.

[115] Pietropaoli, S. 2019. *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in *Il Mulino – Rivisteweb*, Fascicolo 2, pp. 380-397.

Non bisogna dimenticarsi che la geografia variabile del cyberspazio non è altro che l'esito storico della necessità e della volontà di comunicare e ricordare grosse quantità di dati e di memorie, rendendo quindi richiamabili tracce di eventi passati o comunque di esperienze localizzate nel passato[116].

Il fatto che vi sia un continuo e quotidiano ampliamento dei confini dello spazio dei dati digitali e delle cyber-relazioni, porta alla conferma dell'opportunità di inserire l'agire umano dentro un vasto spazio di "tecnaturalità[117]", per il quale si fanno concrete le disposizioni che sono state ereditate per via genetica dagli individui, solo nel momento in cui vengono introdotte in un ambiente mobile artificioso, e che di conseguenza è già un prodotto umano.

Il concetto di "luogo" viene trasferito nel dominio digitale trasformandolo in un "sito", raggiungibile a partire da una propria navigazione: dobbiamo pensare al cyberspazio come ad un dominio digitale costituito da una molteplicità e varietà di reti utilizzate ai fini di scambio e archivio di memorie, un grande paesaggio virtuale formato da questi archivi che vengono continuamente chiusi e riaperti e nel quale le memorie, a seguito della trasformazione dei testi e dopo essere state riposte all'interno di uno specifico archivio, vengono divulgate nelle più varie direzioni, diventando così informazioni utilizzabili e consultabili nei contesti più disparati[118].

4. Il principio di territorialità nel cyberspazio ed i suoi limiti

È ben noto che il cyberspazio sia in grado di travalicare i confini spazio-temporali e che consente di accedere alla rete anche contemporaneamente in più luoghi virtuali, essendo che risulta privo di confini territoriali, o per meglio dire, spaziali.

Gray sostiene che il cyberspazio, pur essendo un ambiente "*placelessness*", è costituito da elementi fisici e digitali che assieme contribuiscono a renderlo allo stesso tempo

[116] Scardovi, G. 2018. *Mondo che genera mondo: memoria, codice, cyberspazio*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 4-23.
[117] Scardovi, G. 2018. *Mondo che genera mondo: memoria, codice, cyberspazio*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 4-23.
[118] Scardovi, G. 2018. *Mondo che genera mondo: memoria, codice, cyberspazio*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 4-23.

reale e virtuale[119]. Nonostante ciò, non è comunque paragonabile al cento per cento allo spazio reale, specialmente facendo riferimento al principio di territorialità, il quale esige nel nostro ordinamento l'individuazione di un luogo in cui è stata realizzata la condotta: tale principio permette l'istituzione di un collegamento tra il fatto e l'ordinamento giuridico corrispondente al luogo in cui è stato commesso, applicando quindi la legge penale a quei fatti che sono commessi nel territorio statale.

L'applicazione del principio di territorialità per individuare il luogo il cui il *cybercriminale* compie l'illecito è problematica: le operazioni che vengono compiute online partono da un luogo ma successivamente si snodano nella rete, non rimangono statiche.

Il principio di territorialità, anche se presenta notevoli difficoltà di applicazione, tuttavia non può essere abbandonato, ma deve piuttosto tenere conto delle specifiche caratteristiche particolari dei reati informatici per l'individuazione di soluzioni che permettano al giurista di collocare in uno spazio preciso l'illecito commesso in Rete.

Sarebbe opportuno adottare un provvedimento sovranazionale che sia in grado di coinvolgere più ordinamenti giuridici possibili ai fini di definire quei criteri che devono essere seguiti per stabilire un collegamento tra l'illecito perpetrato online e l'ordinamento giuridico corrispondente.

Il tratto che distingue i reati informatici in relazione al problema del principio di territorialità è il loro elevato tasso di delocalizzazione, che contribuisce a rendere assai difficile la determinazione del luogo in cui si è realizzata la condotta illecita: la rete è accessibile a tutti da qualsiasi parte del mondo, di conseguenza è quasi impossibile circoscrivere le conseguenze del reato sul piano spaziale[120].

Il fatto che le condotte poste in essere si discostino dalla fisicità che denota i comportamenti tradizionali, rende complessa l'indicazione del luogo in cui il fatto viene commesso e anche l'individuazione del responsabile, che potrebbe sfruttare a suo favore la presenza di *paradisi informatici*, facendo riferimento con questo ultimo termine alla mancanza di una legislazione uniforme che possa sanzionare gli illeciti commessi dai cybercriminali in questo spazio-non-spazio.

---

[119] Martino, L. 2018. *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 61-72.

[120] Braschi, S. 2020. *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, Cedam.

Alcuni Stati per sopperire ai limiti concernenti il tradizionale principio di territorialità ricorrono all'impiego di altri principi ai fini dell'individuazione del *locus commissi delicti* e quindi dell'individuazione della giurisdizione competente: ad esempio in alcuni casi può essere utilizzato il principio di personalità attiva, secondo il quale assume rilevanza la nazionalità del soggetto che pone in essere la condotta.

Sorgerebbero comunque dei problemi anche se si utilizzasse come criterio per l'individuazione del luogo in cui viene commesso il reato il luogo in cui è ubicato il *server*, perché le operazioni si traducono in plurime operazioni che si realizzano fra diversi server localizzati in diversi luoghi, coinvolgendo quindi diversi Stati e di conseguenza diverse giurisdizioni.

È comunque bene precisare che con queste riflessioni non facciamo riferimento ai reati di evento e ai reati informatici per i quali non è necessaria una connessione in rete, ma unicamente ai *cybercrimes* ovvero quei reati informatici che invece tassativamente hanno come presupposto l'utilizzo di una Rete ai fini della commissione dell'illecito.

Con riguardo ai reati cibernetici è necessario ricordare la distinzione tra la perfezione del reato, quindi il momento in cui avviene l'integrazione degli elementi costitutivi essenziali, e la consumazione del reato, che è il momento in cui vi è la massima esplicazione dell'offesa[121]. È importante fare riferimento a questa distinzione perché il cyberspazio con le sue caratteristiche determina la permanenza e la circolazione dei dati e dei contenuti all'interno di esso, quindi il fatto di reato continua a produrre i suoi effetti nel tempo proprio in relazione alle funzioni che, essendo automatizzate, consentono la continua circolazione, messa a disposizione e condivisione. Da qui si evince il problema del prolungamento degli effetti e il fatto che questo prolungamento non può non essere punito: per la maggior parte dei casi il luogo di commissione del reato dovrebbe rinvenirsi nel luogo in cui avviene la prima manifestazione dell'evento o il verificarsi della condotta, ma quando non è possibile stabilire dove sia avvenuta la consumazione è necessario riferirsi all'ultimo luogo in cui è avvenuta parte dell'azione od omissione e qualora anche questo non fosse rintracciabile, ci si dovrà riferire alla dimora, residenza, domicilio del reo[122].

---

[121] Flor, R. 2019. *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in *Cybercrime – Diritto e procedura penale dell'informatica*, Utet, pp. 141-192.

[122] Flor, R. 2019. *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in *Cybercrime – Diritto e procedura penale dell'informatica*, Utet, pp. 141-192.

Ad oggi il problema dell'individuazione del *locus commissi delicti* con riferimento ai *cybercrimes* non ha ricevuto una risposta uniforme: la questione deve essere comunque affrontata caso per caso tenendo conto dei principi del nostro ordinamento giuridico e cercando di interpretarli al fine di fornire delle soluzioni pratiche al singolo caso proiettato sulla dimensione del cyberspazio.

5. *Il ruolo del diritto nella regolazione di Internet*

Come afferma Maestri, la nostra è una società tecnologicizzata: vale a dire che i fini delle nostre azioni sono fortemente influenzati dal panorama tecnologico e che i mezzi utilizzati per inseguire questi nostri fini, sono anche questi tecnologici; risulta quindi che ciò che regola le relazioni fra i mezzi e i fini è proprio la tecnologia[123].

Possiamo affermare che il diritto nel Web sia un diritto *tecnologicizzato*, in cui la tecnica digitale viene assunta come regola ai fini della disciplina dei rapporti digitali[124].

Il tecnico informatico assume un ruolo centrale e fondamentale come fonte di produzione delle regole, pur non essendo investito di nessuna forma di legittimazione democratica ai fini dello svolgimento di questa funzione: la sua legittimazione deriva in automatico dalle conoscenze e dalle abilità tecniche da lui possedute. È lui che crea gli standard su cui si fonda la Rete, delimitando in questo modo i confini d'azione del diritto, facendo assumere a quest'ultimo le caratteristiche della deterritorializzazione, destatualizzazione e dematerializzazione.

La destatualizzazione segna la crisi della sovranità dello stato, in quanto la rigidità del diritto statale risulta incapace di riuscire a regolare le nuove modalità con cui gli umani operano, rendendo così inevitabile la produzione di un diritto flessibile che sia in grado di adattarsi al modello del mondo digitale.

Appare ormai scontato tornare ad affermare che il diritto si stia evolvendo: questo processo di evoluzione sta facendo si che questo stia passando dall'essere un diritto imposto dall'alto all'essere un diritto che risulta sempre più partecipato: tale passaggio

[123] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[124] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

appare dato dal fatto che antecedentemente alla globalizzazione era la "persona" a risultare il fulcro del diritto e di ogni relazione, mentre invece nel contesto del diritto tecnologicizzato è oggi il mercato che tende a sostituirsi alla persona ponendosi al centro di qualsiasi relazione sociale[125]. Maestri sostiene che ad oggi la globalizzazione sia soprattutto una globalizzazione economica.

Di fronte alla globalizzazione il diritto tipico diventa il *soft law*, facendo riferimento con questo termine ad un complesso di tecniche regolative di fonti di produzione contenenti regole di condotta che, anche se scritti, sono privi di forza legale in grado di vincolare; sono però in grado di ottenere effetti concreti e pratici indirizzando e orientando i comportamenti dei rispettivi destinatari. Il *soft law* è un diritto che si adatta ai bisogni della tecnologia[126].

Il diritto è da sempre stato, prima di essere oggetto di applicazione, un oggetto di interpretazione. Nel diritto dei computer la norma prima di essere oggetto di esecuzione diviene oggetto di calcolo: a seguito della traduzione delle norme giuridiche nel linguaggio informatico vi è la necessità di rinunciare poi all'impiego di formule che possano implicare un'attività valutativa *ex post*, con il fine di adottare formule per cui la loro struttura consenta di effettuare valutazioni di conformità (o meno) ad una certa fattispecie astratta formulabile *ex ante*.

La progressiva diminuzione del divario fra norma giuridica e regola informatica a causa dell'algoritmizzazione della prima mette il giurista di fronte ad un interrogativo: "Fino a quando si potrà accettare che la legge scritta come software implichi, sostanzialmente, che il software diventa la legge stessa?[127]".

[125] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[126] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[127] Spedicato, G. 2009. *Law as Code? Divertissement sulla lex informatica*, in *Cyberspazio e diritto*, Vol. 10, pp. 233-259.

6. La proposta di una Costituzione propria del cyberspazio

Il più grande spazio pubblico che l'uomo abbia mai conosciuto, quello spazio astratto che circonda il globo e dal quale siamo ormai dipendenti: stiamo parlando dell'Internet, luogo-non-luogo che non ha sovrano.

John Perry Barlow nel 1966 apriva in questo modo la sua Dichiarazione d'indipendenza del cyberspazio: "Governi del mondo industriale, stanchi giganti di carne e di sangue, io vengo dal Cyberspazio, la nuova dimora della mente. In nome del futuro, invito voi, che venite dal passato, a lasciarci in pace. Non siete benvenuti tra noi. Non avete sovranità sui luoghi dove ci incontriamo"[128].

Con questo tono, a tratti provocatorio, Barlow sembra preannunciarci che a quel tempo stava iniziando a prendere il via l'espansione di una rete di comunicazioni che nessun soggetto sarebbe stato in grado di controllare, di bloccare, né tantomeno di comandare.

Non sono mancate di certo alcune aggressive repliche al pensiero dell'Autore: ai tempi di questa Dichiarazione d'indipendenza del cyberspazio avanzava sempre di più la pretesa da parte degli Stati nazionali di continuare a far valere le loro prerogative (risultanti ormai obsolete) e di proseguire nella considerazione della rete quale "oggetto del desiderio delle sovranità esistenti[129]".

Gli Stati cercano in tutti i modi di imporre la loro presenza: allo stesso tempo però inizia a diffondersi l'idea di un quadro costituzionale che dovrebbe permettere il consenso di una nuova narrazione dei diritti nel mondo del Web, prendendo come punto di partenza le questioni chiave che sono senza dubbio l'accesso come diritto fondamentale e la neutralità della rete.

Dichiarazioni bilaterali iniziano a prendere piede fra gli Stati, le quali dovrebbero essere il buon punto di partenza con la prospettiva a lungo termine di raggiungere iniziative su larga scala.

Sempre più di frequente sentiamo discutere di una possibile *Internet Bill of Rights*, ovvero una Costituzione per la Rete: questo perché si stanno sempre di più affermando dei sistemi di regolazione che si fondano su modelli di autoregolamentazione e *governance* affidati a soggetti privati; notando l'atteggiamento ostile da parte dei

[128] Rodotà, S. 2010. *Una Costituzione per Internet?* , in *Il Mulino – Rivisteweb*, Fascicolo 3, pp. 337-351.
[129] Rodotà, S. 2010. *Una Costituzione per Internet?* , in *Il Mulino – Rivisteweb*, Fascicolo 3, pp. 337-351.

governi nazionali nei confronti di Internet e la sua libertà, pare che sia giunto il momento di formare un'articolazione di garanzie costituzionali per i diritti della Rete e in rete[130].

La scelta dell'impostazione del *Bill of Rights* mette in evidenza che con questa Costituzione non si vuole andare a limitare la libertà in rete, ma anzi si vogliono mantenere le condizioni affinché questa libertà possa continuare a fiorire: è per questo che è indispensabile elaborare delle garanzie "costituzionali"[131].

Quando il cammino verso questa Costituzione diventerà più spedito, vi sarà già stato un cambiamento, e questo cambiamento risiederà nel fatto che si andrà via via affermandosi un nuovo e diverso modello culturale basato sul fatto che il cyberspazio è un universo senza confini, un modello che consentirà di costituire un riferimento per i giudici che affrontano i problemi posti dall'innovazione tecnologica e scientifica: si darà voce a quei diritti fondamentali che ad oggi rappresentano l'unico potere in grado di opporsi alla forza degli interessi economici[132].

L'introduzione di un sistema di regolazione basato su di una Costituzione propria del cyberspazio non andrebbe a valere unicamente contro l'invadenza degli Stati nazionali, ma bensì dovrebbe proiettarsi anche verso le nuove *corporations* multinazionali dell'informazione, che utilizzano enormi banche dati per governare e controllare la vita dei singoli utenti: possiamo definire questa pesante invadenza come uno "strapotere tecnocratico[133]" delle *corporations*, che si andrebbe via via frammentandosi con l'introduzione di un'iniziativa costituzionale.

Il termine "*privacy*", oltre ad evocare un bisogno di intimità, sintetizza anche quelle libertà che ci appartengono in questo nuovo mondo digitalizzato in cui ci troviamo[134].

Questo mondo ha bisogno di una pluralità di attori che possano dialogare al fine di mettere a punto delle regole comuni: soggetti diversi, con strumenti diversi, negoziano e si legano con reciproci impegni al fine dell'individuazione di un patrimonio comune di diritti, rendendolo poi effettivo.

---

[130] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[131] Rodotà, S. 2010. *Una Costituzione per Internet?* , in *Il Mulino – Rivisteweb*, Fascicolo 3, pp. 337-351.

[132] Rodotà, S. 2010. *Una Costituzione per Internet?* , in *Il Mulino – Rivisteweb*, Fascicolo 3, pp. 337-351.

[133] Maestri, E. 2015. *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

[134] Rodotà, S. 2010. *Una Costituzione per Internet?* , in *Il Mulino – Rivisteweb*, Fascicolo 3, pp. 337-351.

Lessing ritiene che la creazione di una Costituzione del cyberspazio sia necessaria soprattutto per fissare quei valori che in Rete necessitano di essere garantiti e protetti: egli vorrebbe garantire Internet in qualità di spazio pubblico che sia controllato da un soggetto garante dei diritti di tutti, e che sia in grado di bilanciare gli interessi in gioco[135].
La questione dell'Internet, definita da Rodotà come un "fiorire di dichiarazioni dei diritti", va presa sul serio, perché individua procedure e soggetti differenti da quelli che sono stati tradizionalmente presenti durante le fasi di istituzionalizzazione dei diritti.
Entriamo in una dimensione non dell'ignoto ma dell'inedito[136], perché di fatto non ci si muove in un ambiente del tutto sconosciuto, ma bensì si tratta di un ambiente pieno di materiali in continua evoluzione, i quali necessitano di comprensione e di analisi, e in quanto processo inedito non lo si può valutare con i criteri del passato.
In conclusione a queste riflessioni, possiamo certamente affermare che, diversamente da ciò che sostengono le impostazioni liberiste, anche Internet può essere oggetto di regolazione e sanzione giuridica.
Il carattere neutrale della Rete deve essere salvaguardato come strumento per consentire la piena esplicazione delle libertà costituzionali[137].
È necessario inoltre dare il via ad un processo di alfabetizzazione digitale che possa permettere a tutti l'esercizio di quelle libertà costituzionali che si possono esplicare mediante Internet.

[135] Lessing, L. 2006. *Code version 2.0*, Basic Books, New York.
[136] Rodotà, S. 2010. *Una Costituzione per Internet?* , in *Il Mulino – Rivisteweb*, Fascicolo 3, pp. 337-351.
[137] Betzu, M. 2012. *Regolare internet. Le libertà di informazione e di comunicazione nell'era digitale*, Giappichelli Editore, Torino.

CONCLUSIONI

Alla luce di tutte le considerazioni e delle riflessioni che sono state fatte nel presente elaborato, possiamo con certezza affermare che il *cyberspazio* può a tutti gli effetti essere considerato come un nuovo *locus commissi delicti*, in cui l'utilizzo dell'anonimato da parte del cybercriminale è in grado di produrre una sorta di effetto inibitorio, che favorisce così l'azione criminale.

Parlare di un argomento così attuale e, a mio parere, così "stravolgente", mi ha affascinata: pensare che oltre al mondo in cui tutti viviamo, esista anche una sorta di realtà parallela costruita interamente *online*, in cui certe azioni che noi comunemente svolgiamo tutti i giorni, si possano svolgere anche in questo mondo digitale senza confini e senza territorio, mi affascina. Sono consapevole del fatto che sia in grado di affascinare quanto allo stesso tempo di spaventare, uno spavento che deriva dal fatto che spesso sentiamo dire che la tecnologia sta prendendo il sopravvento sulle nostre vite, o che l'intelligenza artificiale prima o poi supererà quella umana.

L'uomo ha creato la tecnologia, e ora la tecnologia sta in un qualche modo governando la vita dell'uomo, che si ritrova a fronteggiare delle problematiche che lui stesso ha creato, come appunto il problema della localizzazione dell'illecito compiuto tramite mezzi informatici.

Alla rete Internet vi accedono soggetti da ogni parte del globo ed è praticamente impossibile individuare l'ordinamento giuridico di riferimento da applicare in caso di conflitto.

Il reato informatico è privo di confini, anche detto *borderless*, la quale risulta essere una caratteristica inedita se si opera un confronto con le caratteristiche proprie di quei reati considerati "comuni"; è una peculiarità propria del cybercrime che non trova precedenti nella storia e proprio per questo possiamo affermare che sia il reato del terzo millennio per eccellenza.

Mi trovo in accordo con gli studiosi che sostengono la tesi che prevede la creazione di una Costituzione propria del cyberspazio: il fatto che le azioni poste in essere dai cybercriminali possano avvenire in giurisdizioni separate da enormi distanze, rende difficoltoso il lavoro delle forze dell'ordine, perché ora risulta necessaria una

cooperazione internazionale per regolare quei crimini che in precedenza erano locali o nazionali.

È vero anche che, a seguito di una possibile Costituzione per il cyberspazio, sorgerebbe il problema dell'adozione di questa nei vari Stati, e il fatto di dover elaborare un documento che possa essere accettato a livello europeo o addirittura mondiale (come sarebbe auspicabile) fa sorgere alcuni dubbi a riguardo.

Sarebbe comunque già un buon punto di partenza continuare sulla strada della ratifica di quei trattati internazionali che sono già in vigore da qualche anno e che tuttavia non tutti gli Stati hanno adottato, come ad esempio la Convenzione di Budapest.

È necessario che, quanto prima, l'Unione europea si doti di una normativa specifica in grado di armonizzare le varie legislazioni degli Stati membri e rendere così il più omogeneo possibile l'intervento sui crimini informatici, in particolare in vista della soluzione del problema concernente la localizzazione del crimine, quindi l'applicazione del principio di territorialità. Partendo da un possibile esempio europeo si potrebbe poi, ampliando i confini, raggiungere anche accordi con altri Stati.

La criminalità nel cyberspazio è a tutti gli effetti diventata una delle principali sfide alla sicurezza globale, una sfida che l'uomo deve essere in grado di regolare e soprattutto di vincere: è necessario promuovere la consapevolezza dell'utilizzo di queste nuove tecnologie per limitare il più possibile i rischi di vittimizzazione, soprattutto dei soggetti altamente vulnerabili.

Floridi sostiene che la nostra sia l'ultima generazione a fare esperienza di una nitida distinzione fra ambienti online e offline, e personalmente mi trovo in accordo con il suo pensiero.

La tecnologia sta sempre di più invadendo le nostre vite, e noi dobbiamo riuscire a sfruttare al meglio le opportunità che questa ci offre, tenendo però sempre a mente che le opportunità sono tante quanto i rischi, ed è necessario essere sempre ben consci di questo.

Il cyberspazio è uno spazio comune, e in quanto tale è opportuno tutelarlo a vantaggio di tutti.

BIBLIOGRAFIA

ALBANESE, V. (2022). *La Quarta Rivoluzione Industriale tra Opportunità e Disuguaglianze*, FrancoAngeli s.r.l., Milano.

AMORE, S. (2006). *Internet ed il diritto penale. I crimini informatici: dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Halley Editrice.

APRUZZESE, A. (2010). *Autori e vittime nella criminalità informatica*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. III-IV, pp. 101-106.

BENANTI P., MAFFETTONE S., (2021). "*Sostenibilità D". Le conseguenze della rivoluzione digitale nelle nostre vite*, in *Il Mulino – Rivisteweb*, Fascicolo 2, pp. 192-206.

BETZU, M. (2012). *Regolare Internet. Le libertà di informazione e di comunicazione nell'era digitale*, Giappichelli, Torino.

BLENGINO, C. (2009). *La devianza informatica tra crimini e diritti: un'analisi sociogiuridica*, Carocci, Roma.

BRASCHI, S. (2020). *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, Cedam.

CECCACCI, G. (1994). *Computer crimes*, Fag, Milano.

CAMPA, R. (2007). *Considerazioni sulla Terza Rivoluzione Industriale*, in *Il pensiero economico moderno*, Vol. 3, Pisa.

CASS. PEN., 27 settembre 2013, Sez. I, sent. n. 40303.

CASS. PEN., 26 marzo 2015, Sez. Un., sent. n. 17325.

D'AIUTO, G., LEVITA, L. (2012). *I reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè.

DEL RE, C. (2009). *Formazione di un nuovo fenomeno criminale: i reati informatici. La frode informatica*, Edizioni Polistampa, Firenze.

DI DONATO, M. (2022). *La Quarta Rivoluzione Industriale tra Opportunità e Disuguaglianze*, FrancoAngeli s.r.l., Milano.

DI FEDE, C., CORRADINI, I, (2004). *La Criminalità informatica: un'analisi socio-criminologica*, in *Tecnologie dell'Informazione e Comportamenti Devianti*, LED Edizioni Universitarie.

FLORIDI, L. (2017). *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano.

FLOR, R. (2019). *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in *Cybercrime – Diritto e procedura penale dell'informatica*, Utet, pp. 141-192.

FORTE, F. (2016). *Il cyberspazio tra governamentalità e digitalità*, in *La Deleuziana – Rivista Online di Filosofia*, n. 3, pp. 87-101.

GALDIERI, P., CORRADINI, I., (2004). *La Criminalità informatica: un'analisi socio-criminologica*, in *Tecnologie dell'Informazione e Comportamenti Devianti*, LED Edizioni Universitarie.

IRTI, N. (2006). *Norma e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari.

IRTI, N., SEVERINO, E. (2001). *Dialogo su diritto e tecnica*, Laterza, Roma-Bari.

KOBRIN, S. J. (2001). *Territoriality and the Governance of Cyberspace*, in *Journal of International Business Studies*, Vol. 32, pp. 687-704.

LAZZERONI M., ZAMPERLIN P., (2022). *La Quarta Rivoluzione Industriale tra Opportunità e Disuguaglianze*, FrancoAngeli s.r.l., Milano.

LEONHARDT DOS SANTOS, D. (2019). *A territorialidade no contexto da criminalidade global: considerações sobre a influência do ciberespaço na delimitação jurisdiccional*, in Rev. Bras. De Direito Processual Penal, Porto Alegre, Vol. 5, pp. 597-622.

LESSING, L. (1999). *Code and Other Laws of Cyberspace,* Basic Books, New York.

LESSING, L. (2006). *Code version 2.0*, Basic Books, New York.

MAESTRI, E. (2015). *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, Napoli.

MAESTRI, E. (2017). *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 15-26.

MAROTTA, G. (2012). *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, in *Rivista di Criminologia, Vittimologia e Sicurezza* – Vol. VI, pp. 94-106.

MARTINO, L. (2018). *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 61-72.

MATTARELLA, A. (2022). *La futura Convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, in *Sistema Penale*, Fascicolo 3, pp. 60-102.

MINGARDO, L. 2020. *Il diritto delle macchine. Tecnodiritto e intelligenza artificiale in una prospettiva critica di informatica giuridica*, in *Anthropologica*, pp. 51-64.

MORO, P. 2019. *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *MediaLaws – Rivista di diritto dei media*, pp. 12-22.

MURRAY, A. (2003). *The Regulatory Edge of the Internet*, in *International Journal of Law and Information Technology,* Vol. 11, pp. 87-97.

MURRAY, A. (2011). *Nodes and Gravity in Virtual Space*, in *Legisprudence*, Vol. 5, Routledge, pp. 195-221.

PANATTONI, B. (2019). *Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online*, in *Diritto Penale Contemporaneo - Rivista Trimestrale*, Vol. 2, pp. 35-52.

PARIOTTI, E. (2004). *La giustizia oltre lo stato: forme e problemi*, Giappichelli, Torino.

PICOTTI, L. (2008). *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, Fascicolo 5, pp. 437-448.

PIETROPAOLI, S. (2019). *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in *Il Mulino – Rivisteweb*, Fascicolo 2, pp. 380-397.

RODOTÀ, S. (2010). *Una Costituzione per Internet?* , in *Il Mulino – Rivisteweb*, Fascicolo 3, pp. 337-351.

SARRA, C. 2018. "*Iper positività": la riduzione del giuridicamente lecito al tecnicamente possibile nella società dell'informazione*, in *JusQuid – sezione scientifica*, pp. 95-122.

SCARDOVI, G. (2018). *Mondo che genera mondo: memoria, codice, cyberspazio*, in *Il Mulino – Rivisteweb*, Fascicolo 1, pp. 4-23.

SPEDICATO, G. (2009). *Law as Code? Divertissement sulla lex informatica*, in *Cyberspazio e diritto*, Vol.10, pp. 233-259.

STRANO, M. (2001). *Relazioni digitali e comportamenti devianti*, Relazione al convegno "Psichiatria informatica e telemedicina. Realtà e prospettive nel campo dell'assistenza della formazione", Velletri.

TONELLOTTO, M. (2022). *Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. XVI, pp. 7-19.

VULPIANI, D. (2007). *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*, in *Rivista di Criminologia, Vittimologia e Sicurezza* Vol. I, pp. 1-9.

WENGUANG, Y. (2018). *Internet Intermediaries' Liability for Online Illegal Hate Speech*, in *HeinOnline Law Journal Library*, Vol. 13, pp. 342-356.

SITOGRAFIA

www.agendadigitale.eu

www.altalex.com

www.cybersecitalia.it

www.cybersecurity360.it

www.corrierecomunicazioni.it

www.dirittogiustiziaecostituzione.it

www.europarl.europa.eu

www.ilsole24ore.com

www.iusinitinere.it

www.lucidamente.com

www.poliziadistato.it

www.salvisjuribus.it

www.sistemapenale.it