UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO

CORSO DI LAUREA IN

CONSULENTE DEL LAVORO

A.A. 2021-2022

IL CONCETTO DI LEX INFORMATICA NEL DIBATTITO TRA CYBERPATERNALISM E CIBERLIBERTARIANISM

Relatrice: Prof.ssa Mingardo Letizia

Laureanda: Bicciato Anna

Matricola: 1199160

“Anche quando avremo messo a posto tutte le regole,
ne mancherà sempre una:
quella che dall’interno della sua coscienza
fa obbligo a ogni cittadino di
regolarsi secondo regole”

Indro Montanelli

INDICE

INTRODUZIONE

L' intento dell'elaborato è quello di dare inizialmente una visione generale della Lex informatica per poi affrontare il dibattito tra cyberpaternalism e cyberlibertarianism ed in fine analizzare il fenomeno del crimine informatico organizzato.

Nel primo capitolo viene presentata la definizione di Lex informatica, ovvero tutto quell'insieme di norme che regolano la rete, ed il suo ambito di applicazione. Essa permette di stabilire delle specifiche norme per i flussi di informazioni che transitano sulla rete. Tali norme sono destinate a regolare fenomeni che hanno un forte impatto sull'individuo che si vede condizionato nell'esercizio della propria libertà e diritti fondamentali.

Si va poi ad esaminare la fonte del diritto della Lex informatica, ovvero il concetto di Code secondo l'analisi di Lawrence Lessig; verranno esposte le caratteristiche del Codice, che va a costituire l'architettura della rete, le sue funzioni, come gli stati possono andare ad intervenire sul codice per cercare di regolamentare il cyberspazio e quali possono essere i problemi connessi al Code e all'architettura.

Verranno anche messe in luce e spiegati, quali secondo Lessig sono gli strumenti che indirettamente e direttamente possono intervenire sulla regolamentazione dei comportamenti.

Esaminando la questione riguardante la governance di internet, andiamo ad esporre come viene gestita la governance a livello internazionale e quali strumenti ed istituti, come ad esempio l'ICANN, come la sua gestione, e regolamentazione. Si andrà ad esporre cos'è l'ICANN, quale sia il suo scopo e le sue funzioni.

Si parlerà di Internet come luogo di libertà, caratterizzato da un'assenza di confini dove tutto è libero e di conseguenza luogo in cui possono manifestarsi comportamenti illeciti.

È stata anche brevemente analizzata l'evoluzione (passaggio da web 1.0 a 3.0) che il web ha avuto nel tempo, per consentire la creazione di un'interazione tra utente e contenuto.

Proseguirò poi con l'analisi della teoria di J.R. Reidenberg, la quale vede messe a confronto la regolamentazione giuridica e la Lex Informatica, in tutti i suoi profili.

Nel secondo capitolo, affronterò la questione della regolabilità o meno del cyberspazio nel dibattito tra cyberpaternalismo e cyberlibertarianismo.

Vengono messe in evidenza le ideologie dei sostenitori del cyberlibertarianismo, partendo da un piccolo accenno a cosa sia il libertarismo e quali siano i suoi principi, citando il pensiero di uno dei suoi maggiori esponenti, M. N. Rothbard; vivi e lascia vivere è il motto del cyberlibertario, il quale sostiene che libertà economica e libertà sociale siano intrecciate tra loro. Vengono esposte la visione pessimistica e ottimistica del cyberlibertarismo.

Successivamente vengono esposte le ideologie del cyberpaternalismo, evidenziandone le differenze e le ideologie contrapposte al cyberlibertarismo, facendo anche riferimento all'operato sulla Lex informatica di J.R. Reidenberg ed all'individuazione da parte di Lawrence Lessig, delle quattro forze normative che agiscono sugli individui che operano all'interno del cyberspazio. È stato proprio grazie a questi lavori che la prospettiva cyberpaternalista si è evoluta ed è cambiata. Ci si è anche soffermati su come viene regolato il cyberspazio secondo l'ottica cyberpaternalista e cyberlibertarianista.

Per concludere mi sono soffermata ad analizzare il fenomeno del crimine informatico, in generale esponendone la nozione, quali sono gli strumenti di contrasto e il problema legato alla territorialità (accenni al principio di territorialità in materia penale).

In Italia, uno dei segnali che ha fatto comprendere, la volontà dello stato di combattere questo fenomeno è stata la ratifica con la l. 18 marzo 2008, n. 48 della Convenzione sulla criminalità informatica di Budapest del 2001; mette a livello europeo un segnale di contrasto è stato l'emanazione della direttiva europea 2013/40/UE, con la quale l'unione europea ha evidenziato anche il rapporto che c'è con il crimine organizzato. Proprio in riferimento a quest'ultimo, è stato presentato un confronto tra criminalità informatica e crimine organizzato e sono stati riportati alcuni casi di criminalità organizzata informatica che hanno visto come protagonisti, alcune organizzazioni di stampo mafioso come l'Ndrangheta ma anche organizzazioni di stampo mafioso operanti al difuori dello stato italiano.

Sono stati poi messi in luce gli aspetti problematici che si riscontrano tra diritto positivo e criminalità informatica quali: le difficoltà di inquadramento dell'illecito informatico, la penalizzazione di tali comportamenti illeciti e le difficoltà legate alla territorialità.

In fine è stato, sempre collegandosi al crimine organizzato informatico mi sono soffermata sull'esporre cosa sia il COC (Cyber Organized Crime) con riguardo alla classificazione del cyber organized crime che si ottiene tenendo conto della natura e delle caratteristiche dell'attività criminale.

CAPITOLO 1

LEX INFORMATICA

1. Definizione ed ambito di applicazione della Lex Informatica.

La Lex Informatica costituisce l'insieme di norme che regolano la rete. Permette di stabilire norme specifiche per i flussi di informazioni, veicolati sulla rete e di imporre politiche generali dei flussi e di automazione delle informazioni digitali.

Si tratta di norme invisibili ad occhio nudo, che regolano fenomeni che si collocano al di là della percezione e comprensione di coloro che ne subiscono le conseguenze. Tali fenomeni non rimangono neutrali, al contrario esercitano un forte impatto sull' individuo, che sarà condizionato nell' esercitare le proprie libertà e i propri diritti fondamentali e possono influenzare anche la formazione delle decisioni pubbliche.

Essa inoltre definisce anche l'Internet of Things, le piatteforme come Facebook, Instagram, Twitter e TikTok, sulle quali molti esprimono la loro personalità, ovvero i metadati, che consentono a calcolatori estremamente veloci di gestire domanda e offerta di un mercato pubblicitario dominato da pochissimi.[1]

Il Global Internet report della Internet Society del 2019, riporta una illustrazione della Internet Economy, composta da tre settori interconnessi tra di loro, che dialogano e si condizionano a vicenda. Delle venti società maggiormente capitalizzate nel mondo undici di queste sfruttano la rete, essendo lei prima di tutto economia, ottenendone ricavi onerosi.

La Lex informatica oltre a rendere possibile materialmente questo fenomeno gli da anche una direzione.

Ci si chiede se il Volunteer core della Lex informatica è veramente animato da uno spirito così benevolo da rendere veramente migliore la rete rispetto a come è stata trovata.

I tre settori di cui è composta la rete sono: il backcone: cioè l'infrastruttura, regolata dal diritto delle telecomunicazioni, che si presenta come un diritto orientato verso le macchine; i calcolatori: che collocano la banda sfruttando le potenzialità dell'intelligenza artificiale in termini comprensibili agli umani; i programmatori delle macchine.

---

[1] G.L. CONTI, *La Lex informatica, in Osservatorio sulle fonti*, n 1/2021. Disponibile in: http://www.osservatoriosullefonti.it

L'infrastruttura è un insieme di collegamenti fra nodi, che permettono il collegamento fra punti terminali e il diritto di questa trova fondamento negli accordi in seno all'ITU (Unione Internazionale delle Telecomunicazioni).[2]

Gli ISP (Internet Service Provider) che costituiscono la colonna portante della rete, consentono l'accesso ai punti terminali di rete; ciascun nodo della rete attribuisce ai propri utenti un indirizzo IP, che consente di costruire un web della sorveglianza nel momento in cui l'ISP li rende disponibili ai fini di marketing.

Le applicazioni consentono di utilizzare la rete, con il fine di permettere a chi vi accede di soddisfare le proprie esigenze. Vengono viste come un "luogo" dove l'esperienza della rete va a sostituire la realtà della vita e delle relazioni.

Con riguardo all'accesso e agli standard, che permettono di sviluppare gli applicativi necessari a consentire la comunicazione END TO END, la democrazia della rete è gestita da un insieme di organismi: ICANN che si occupa di gestire gli indirizzi IP e il DNS con una funzione di governo; W3C amministra l' HTML e sviluppa gli standard del World Wide Web; per ultimo abbiamo l' IETF, che va a definire i protocolli che permettono di sfruttare i principi della comunicazione END TO END in nuove direzioni.

2. Fonti del diritto e Code

Internet è un insieme di standard per la trasmissione, lo smistamento e la ricezione di messaggi; la tecnologia, va a condizionare, non solo le modalità attraverso le quali avviene la trasmissione delle informazioni ma anche le scelte che condizionano la disciplina del rapporto assumendo a fonte di vero e proprio rulemaking.

Il rapporto fra diritto e architettura emerge come il perno centrale nella configurazione dei comportamenti possibili nel cyberspazio.[3]

L'architettura digitale è costituita da un Codice, termine con il quale Lessig fa riferimento allo strumento costituito da software, hardware, algoritmi, codici binari attraverso i quali, i programmatori informatici, stabiliscono i modi d'uso della tecnologia informatica, strutturando e architettando la rete.

Il Code produce la trasduzione informatica della legislazione, che si trasforma in uno spazio giuridico elettronico globale. Questo non vuol dire che gli stati non possano andare

[2] G.L. CONTI, *La Lex informatica, in Osservatorio sulle fonti*, n 1/2021. Disponibile in: http://www.osservatoriosullefonti.it

[3] M. GOLDONI, *Politiche del codice. Architettura e diritto nella teoria di Lessig*, cit. p. 5.

a regolare il cyberspazio, ma significa che questi possono regolamentare il cyberspazio andando ad intervenire sul codice e sull'architettura del sistema.[4]

Non possiamo definirlo una vera e propria legge sottoposta a limiti costituzionali, ma possiamo dire che ha la copertura della legge e al tempo stesso può avere maggiore efficacia della stessa. Il Codice viene scritto; la sua scrittura viene messa in atto con lo scopo di raggiungere una visione precisa dello spazio digitale che si vuole creare.[5]

L'architettura però presenta alcuni problemi; trovandoci in un quadro dove l'architettura può risultare decisiva nel andare a disciplinare uno spazio, diventa di rilevante importanza, per la protezione dei valori al suo interno, il controllo dell'operato degli architetti; nel cyberspazio la possibilità di intervenire in maniera architettonica presuppone la possibilità di agire sul codice, e per questo la proprietà e il tipo di licenza, con il quale il software viene venduto o utilizzato diventa una questione decisiva per la configurazione dell'ambiente cibernetico[6]

Il secondo problema riguarda la trasparenza degli interventi architettonici; le misure architettoniche non sempre rendono visibili la regolamentazione di un comportamento. Nelle misure architettoniche, le ragioni che spingono il tecnico a promuovere il progetto e che stanno alla base di esso e ne costituiscono la ratio, non sempre sono evidenti ma possono rimanere nascoste o non venire percepite. Si viene quindi a creare una mancanza di trasparenza che comporta una crisi di legittimità dei provvedimenti.

Il code è anche una forma di espressione del soft law, ovvero quell'insieme di atti eterogenei per origine e natura, che nonostante siano privi di effetti giuridici, hanno comunque rilevanza giuridica.

Lessig sostiene anche che, debbano essere sottoposte agli stessi limiti, non solo le disposizioni normative per la difesa del copyright, ma anche le misure protettive del codice, stabilite dal DMCA. Questi sostiene che come è previsto un fare use per il copyright, debba essere previsto un fare use anche per le misure di protezione previste dal DMCA.

---

[4]E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

[5]M. GOLDONI, *Politiche del codice. Architettura e diritto nella teoria di Lessig*, cit. p. 5.

[6]M. GOLDONI, *Politiche del codice. Architettura e diritto nella teoria di Lessig,* cit. p. 6.

Grazie al DMCA, attualmente il codice è in grado di generare una struttura para-giuridica, che gli permette di raggiungere limiti che il copyright non è in grado di raggiungere, per effetto dei vincoli che gli vengono posti dalla Costituzione.

Le possibilità dell'utente, di operare liberamente e consapevolmente nella rete, si riducono, per effetto della complessità della sequenza di bit, che va a costituire l'essenza del software e dei protocolli, ovvero di quei rapporti digitali disciplinati dalla tecnica digitale.

La figura del tecnico informatico acquista un ruolo centrale come fonte di produzione delle regole. Nonostante non sia legittimato democraticamente per lo svolgimento di questa funzione comunque tale legittimazione gli deriva dalla conoscenza e dalle abilità che il tecnico possiede. Questo creando gli standard sui quali si basa la rete, va anche a definire i confini d'azione del diritto e dei diritti.

Grazie a tutto questo il diritto assume un nuovo aspetto, diventa un diritto deterritorializzato, destatualizzato e dematerializzato; la destatualizzazione porta il diritto, a diventare un diritto flessibile, che finisce per adattarsi al modello reticolare del mondo digitale.

A livello transnazionale ed internazionale si è creata una rete di attori globali che concorrono alla creazione del diritto, andando così a sottrarre la potestà legislativa agli Stati nazionali.[7] Causa dell'erosione delle quote di sovranità statali è stata la crisi identificativa tra stato e diritto, che ha portato all'assegnazione di un carattere territoriale al diritto (territorio sovranità statale).

Nell'era della globalizzazione invece la territorialità viene sostituita dalla spazialità, cioè la categoria con la quale il diritto ha affrontato l'interconnessione[8].

Possiamo dire che sia la Lex informatica, a darci le regole tecniche per la realizzazione dell'interconnessione, poiché l'operazione generativa di spazio e la virtualizzazione infinita delle pratiche sociali, sono garantite dalla tecnologia attivata dal code.

La forma dello stato e la teorizzazione delle fonti del diritto si sono evolute: siamo passati ad un modello opposto di gerarchia delle fonti, se prima questo era un modello piramidale, adesso non vi è più un vertice, ma siamo difronte ad una rete di fonti e soggetti che sono legittimati a creare diritto, che si relazionano tra di loro sulla base della realtà da normare

[7]E. MAESTRI, *Lex Informatica e soft law. Le architetture normative del cyberspazio,* settembre 2017.
[8]E. MAESTRI, *Lex Informatica e soft law. Le architetture normative del cyberspazio,* settembre 2017.

e nel quale si riorganizza la gerarchia delle fonti del diritto in modo orizzontale e trasversale.[9]

Dalla struttura delle fonti, che ad oggi regola Internet, possiamo notare che vi è una forma di governo tecnocratico della Rete, che si sottrae ad un controllo di tipo democratico da parte degli stati.

Sia la rete informatica, che quella giuridica esprimono la dimensione della potenzialità e nella porosità del suo tessuto, riflette il ruolo centrale dell'attività del giudice a tutela dei diritti della persona nel web. Nel caso della Lex informatica però si deve evitare che il principio di performatività abbia la meglio sul principio di legalità.

Tecnologia e diritto, nel nuovo mondo digitale, non sono entrati in completa simbiosi, in quanto pare che la tendenza della tecnica, sia quella di assumere un ruolo centrale nella creazione del diritto; da un lato per quello che riguarda le tecnologie informatiche la relazione che intercorre tra attori, azioni e giustizia si manifesta attraverso logiche bottom-up, ovvero logiche aggregative e comunitarie tipiche del web; l'altro lato dell'era dell'informazione è caratterizzata invece da una lotta per il dominio della Rete, che viene messa in atto attraverso la gestione ed il controllo di internet da parte di una corporate governance multi-stakeholders.

Rispetto al modello teorico, secondo il quale la Lex Informatica, rappresenta un solido esempio del passaggio di paradigma "dalla piramide alla rete" dei modi di produzione del diritto e delle giurisdizioni, si va ad integrare un nuovo modello di segmentazione comunicativa che va a trasformare la rete, in una molteplicità frammentata di reti e di sottoreti, non tutte equamente collegabili ed accessibili. Da qui viene in rilievo l'espressione coniata da Lawrence Lessig "Code is Law" dimostra come le architetture tecnologiche di Internet contengono codici e linguaggi normativi auto-organizzativi che stabiliscono e controllano le regole per l'accesso e per l'uso delle informazioni disponibili in rete.

Lawrence Lessig con le sue opere ha influenzato la teoria del diritto contemporaneo.

Nel Novecento, la teoria del diritto, si è soffermata molto sulla regolamentazione dei comportamenti.

[9]E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

Lessig prende in considerazione quattro strumenti che direttamente o indirettamente, possono intervenire nella regolamentazione dei comportamenti.
Il primo degli elementi è proprio, il diritto, che rimane comunque il mezzo più importante per intervenire direttamente sui comportamenti ma indirettamente sugli altri fattori di regolamentazione ed è lo strumento fondamentale per la formazione ed il controllo degli spazi individuali.
Il secondo strumento è rappresentato da quelle che Lessing considera, norme sociali e morali. Le norme sociali sono un aspetto essenziale per il gruppo sociale. Rispetto alle regole giuridiche, le norme sociali, nonostante siano entrambe contraddistinte dalla minaccia della sanzione, vi è una differenza per quello che riguarda l'ambito di applicazione. Le norme sociali vengono messe in atto dal gruppo di appartenenza per mezzo di diversi strumenti.[10]
Terzo elemento è costituito dal mercato. Il mercato applica dei prezzi, attraverso il pagamento dei quali possiamo ottenere beni e servizi. Questo gli permette di controllare l'accesso o la possibilità di compiere determinate azioni.
Il quarto strumento è l'architettura. Questa costituisce la natura di un contesto che può essere modificata per rivedere l'assetto organizzativo dello spazio interessato.
L'idea che il codice sia considerato il diritto permette di mettere in evidenza degli aspetti importanti.
Ad esempio, l'analisi dell'assetto proprietario del software ha portato alla luce un nucleo problematico autonomo rispetto alla tradizione di altre discipline.
Il secondo problema ha ad oggetto la configurazione da parte del diritto degli assetti proprietari dei beni immateriali e del loro impatto sulla cultura. Una delle soluzioni prende la disciplina della proprietà intellettuale. È in questa circostanza che tutta una nuova serie di licenze che prendono il nome di Creative Commons.

Lessig, sostiene anche che il codice del cyberspazio, sta subendo dei cambiamenti e nel momento in cui questo codice cambierà, di conseguenza cambierà anche il carattere del cyberspazio.
I protocolli TCP/IP rendono possibile lo scambio di dati tra le reti senza che queste possano conoscere il contenuto dei dati scambiati e senza che sapere chi si il mittente un

[10] M. GOLDONI, *Politiche del codice. Architettura e diritto nella teoria di Lessig.*

determinato bit di dati. Le caratteristiche del TCP/IP rendono più complessa la regolamentazione del comportamento proprio perché essendo difficile risalire a chi sono le persone, di conseguenza risulta difficile risalire anche al comportamento dell'individuo. Sotto un primo punto di vista questa caratteristica viene considerata una virtù perché protegge la libertà di parola. In altri contesti invece non è così.

Il commercio su internet in futuro sarà uno dei più grandi contesti di regolamentazione. Qui l'architettura non consente transazioni sicure, è molto facile nascondere la fonte di interferenza. In un contesto come il commercio, quella che prima veniva vista come una virtù, verrà invece vista come un interferenza, con la capacità del commercio di progredire.

Ci sono e stanno nascendo, però, architetture che possono aiutare nella regolamentazione del comportamento in rete; ad esempio, le architetture per facilitare l'identificazione o per certificare fatti sull'utente.

3. La Governance di Internet.

La governance di Internet è diventata una delle pratiche di governo più diffuse, soprattutto nel contesto internazionale[11].

L'adozione di standard e di buone pratiche, la cui fine è l'efficienza della burocrazia di un paese, è una delle tecniche di governance maggiormente utilizzate.

Lo scopo della governance è quello di coordinare sia la gestione dei fenomeni globali di carattere tecnico o scientifico che l'amministrazione delle dinamiche politiche in corpo alle organizzazioni internazionali.

Secondo la sociologa Saskia Sassen, la disputa riguardante internet e la sua governance si divide sulla questione che essa sia o meno governabile. Secondo alcuni autori, internet potrebbe essere assoggettata ad un meccanismo di governo, secondo altri invece si presta ad un coordinamento di standard e di regole tecniche.

Assume così importanza, il ruolo che hanno le tecnologie nel determinare possibilità o forme di governance o coordinamento.

[11] E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

Il conflitto che si è creato tra, soggetti pubblici e soggetti privati e tra singoli e governanti nazionali, che ha ad oggetto il controllo del mezzo, è uno degli aspetti essenziali della governance di internet.

Ad oggi la rete è considerata uno dei più rilevanti mezzi di comunicazione. La diffusione di essa ha apportato si grandi vantaggi ma ha comportato anche il sorgere di rilevanti problematiche giuridiche, che vanno dal diritto d'autore alla tutela delle libertà fondamentali e dalla protezione della privacy al controllo sul contenuto delle informazioni. Qui diviene centrale il sistema dei nomi a dominio e la gestione di questi è considerata un modo per controllare il funzionamento di Internet.

L'attività che viene svolta dall' ICANN va a produrre effetti su utenti ed operatori di ogni parte del mondo.

All' ICANN svolge le funzioni essenziali per il funzionamento della rete: *assegnazione e gestione dei nomi di dominio e degli indirizzi IP*, che sono volte a regolare le richieste di appropriazione degli operatori e a determinare gli standard su cui poggia l'intero sistema; *e dei protocolli internet e la supervisione dei root server*, quest'ultimi sono centri che amministrano il vertice della struttura gerarchica dei nomi a dominio. Uno in particolare prevale sugli altri: il root autority ovvero, il potere di dare ordini in merito all'assegnazione dei numeri di dominio e di fare in modo che vengano eseguiti.

Attraverso il controllo della radice l'ICANN è diventata un'autorità centrale.

Inizialmente l'ICANN era organizzato con un sistema a cascata: ad esso spettava la supervisione dei registri e questi a loro volta avrebbero preso accordi con i conservatori del registro, in maniera autonoma e separata; invece, nel sistema attualmente in vigore ci sono registri che operano a scopo di lucro. L'ICANN ha concluso contratti con i registri e con i conservatori.

Le funzioni dell'ICANN sono considerate tecniche ed ha il potere di autorizzare le società ad operare con un determinato nome a dominio con effetti sui diritti degli operatori.

Sul versante organizzativo l'ICANN ricopre contemporaneamente la figura di corporation, ente di standardizzazione e organo di governo.

Può essere classificato una istituzione globale grazie ad alcune principali caratteristiche: presenta una struttura atipica e si conferma la presenza di un sistema multi-organizzativo nell'ordinamento sovrannazionale. Nonostante questo eserciti la sua attività su scala

mondiale e interessa ampio di utenti è un ente privato ma le sue funzioni hanno rilevanza globale.

Secondo aspetto riguarda, il sistema di regole, che pone la sua base sul diritto privato e presenta un carattere periferico che rappresenta un esempio delle nuove forme di "law making".

Terzo aspetto, può essere riconosciuto come un nuovo regime regolatorio internazionale, proprio per il fatto che governa una risorsa vastissima, adotta regole con effetti su scala mondiale dispone strumenti e utilizza processi decisionali per la regolazione dell'intero settore.

Quarto aspetto, il regime dell'ICANN sovrasta il regime degli stati nazionali, perché nel momento in cui le norme che vengono preposte alla regolazione di internet si rivolgono alle parti private.

4. Un luogo di libertà

Oggi ci troviamo difronte a tecnologie della libertà e del controllo. Internet è considerato un luogo di libertà senza confini, del controllo senza governo, del consenso senza potere, questo determina spesso conflitti, la cui soluzione va affidata a norme e a regolamenti oppure a codici di comportamento[12]. La natura del cyberspazio è libertaria e per questo si può dare vita ad una rete che non si può bloccare o controllare.

Internet è una forma di commons, un bene comune, gratuito, formato sia da norme che dalle architetture tecnologiche. La tecnologia informatica nella sua prima parte si dispiega attraverso una logica bottom up, come codice aperto di contenuti, come spazio aperto di conoscenze, un commons che connette tra loro le persone, con vincoli leggeri[13].

Inizialmente ebbe origine quello che ad oggi viene chiamato WEB 1.0., chiamato anche l'internet dei contenuti. Il loro scopo era quello di informare gli utenti senza che si creasse una interazione tra l'utente e il contenuto. I siti si presentavano come enormi libri con pagine che contenevano ipertesti, pagine che contenevano anche immagini o video.

L'impossibilità, che si era creata per l'utente, di interagire con i contenuti, ha costretto i programmatori a rendere il web un luogo dinamico. Da qui ha avuto inizio la

[12]E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

[13]E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

trasformazione del web: si è partiti con la possibilità di inserire commenti; successivamente si è deciso di dare vita a dei forum ed ai primi blog.

Successivamente si è cercato di arrivare a favorire l'interattività con l'utente grazie all' evoluzione di social network, la creazione di community e l'introduzione dei wiki. Si è dato così vita al Web 2.0 ovvero il web dinamico. Il Web però ha continuato ad evolversi, infatti si può dire che stiamo già entrando nel Web 3.0.

Questo bene comune presenta tre aspetti fondamentali quali: il *Codice*, il *commons di conoscenza,* quindi quello scambio di idee e informazioni che riguardano il funzionamento della Rete e del Code, ed il *commons di innovazione,* ovvero l'opportunità che viene data agli utenti di poter innovare e costruire la piattaforma del network. Il code è performativo e da questo possiamo imparare sia leggendolo che applicandolo.

Il commons è una risorsa per l'innovazione centralizzata[14]. I protocolli della rete spronano ad innovare.

Secondo Maestri si potrebbe vedere la rete come un sistema a strati: uno strato fisico, ovvero il computer attraverso il quale viaggiano le informazioni; Il secondo strato, il codice ed i vari protocolli che permettono all' hardware di funzionare; ed in fine il terzo strato che è il contenitore di tutto ciò che viene trasmesso. In questi tre strati, libertà e controllo si alternano. Lo strato fisico, il computer, e lo strato del contenuto non sono del tutto liberi ma vengono controllati.

5. Reidenberg: distinguere Lex informatica dalle norme legali.

Joel R. Reidenberg nella prima parte del suo articolo, "Lex informatica: la formulazione delle regole della politica dell'informazione attraverso la tecnologia", offre un cenno informativo preliminare riguardante le risposte tecniche e le soluzioni, inerenti a problemi politici quali: la regolamentazione legale dei contenuti, delle informazione personali e della proprietà intellettuale sulle reti globali. Queste riflessioni gli hanno permesso di introdurre una teoria di Lex Informatica. In queste infrastrutture per le interazioni umane nazionali e transazionali, le c.d. reti globali, la circolazione delle informazioni personali, la distribuzione della proprietà intellettuale e la regolamentazione dei contenuti sulle reti

[14]E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

hanno fatto sorgere conflitti per il diritto nazionale e internazionale. Allo stesso tempo però la tecnologia ci offre anche delle soluzioni.

Il primo problema che analizza è quello del CONTENUTO, al quale si è cercata soluzione tramite la PICS (piattaforma per la selezione tecnica dei contenuti Internet).

Tale soluzione è stata progettata per porre rimedio al problema di accogliere standard per i contenuti senza andare pregiudicare i valori della libertà di parola.

PICS, consente di facilitare il blocco selettivo dell'accesso alle informazioni su Internet e per fornire un'alternativa alle restrizioni legai della diffusione dei contenuti su Internet.

Essendo un sistema di tecniche che creano uno standard formato per le etichette di classificazione che descrivono i materiali disponibili su internet, viene ad esempio offerto ai genitori uno strumento per andare ad oscurare materiali inappropriati ai loro figli.

Il secondo problema affrontato è quello delle INFORMAZIONI PERSONALI.

Le autorità europee, deputate alla protezione dei dati hanno il potere, di bloccare, impedire i flussi di dati transfrontalieri nel caso la destinazione di questi non rispetti la riservatezza

Nel caso in cui, non fosse rispettata la riservatezza delle informazioni, le autorità europee, deputate alla protezione dei dati, hanno il potere di impedire i flussi di dati transfrontalieri.

Si è cercato di porre rimedio a questo problema, attraverso meccanismi tecnologici, come ad esempio: i remailer anonimi per la posta elettronica oppure i browser anonimi per la navigazione in Internet, che permettono agli utenti di avere un controllo delle loro informazioni personali.

Il terzo problema analizzato da Reidenberg è quello dei DIRITTI DI PROPRIETÀ. Grazie alla tecnologia si è potuto trovare delle risposte ai problemi di ordine giuridico collegati alla gestione dei diritti di proprietà intellettuale.

Con riguardo all'applicazione dei regimi quali il brevetto, il diritto d'autore e il segreto commerciale sono sorti problemi che risultano essere simili a quelli che sono stati riscontrati nella, regolamentazione della privacy, sia dei contenuti che delle info.

Risulta difficile tutelare anche la proprietà intellettuale, delle opere multimediali digitali, in quanto queste possono essere facilmente modificate o alterate dai destinatari.

A fronte di questi problemi viene data possibilità, ai produttori di proprietà intellettuale, di scegliere la tipologia di protezione che ritengono più appropriata. Una tipologia di protezione che può essere adottata dagli autori è quella della protezione della copia.

Questo quadro, di risposte tecniche e soluzioni, alle quali ci troviamo difronte, ha permesso di mettere in evidenza l'esistenza di nuovi modi, per stabilire regole di flussi di informazione. Sono proprio queste soluzioni a dimostrare che le regole per l'accesso e l'utilizzo delle informazioni, sono imposte dalle tecnologie di rete.

Tali imposizioni sui flussi di informazioni forniscono due tipi di regole sostanziali: POLITICHE IMMUTABILI incorporate negli standard tecnologici che non possono essere modificati e POLITICHE FLESSIBILI integrate nell'architettura tecnica che consentono variazioni sulle impostazioni predefinite[15].

Nell'elaborare la sua teoria sulla Lex Informatica, Reidenberg, decide di porre a confronto: la regolamentazione giuridica e la Lex Informatica.

	Regolamentazione giuridica	**Lex Informatica**
Struttura	Legge	Standard di architettura
Giurisdizione	Territorio fisico	Rete
Contenuto	Espressione legale/giudiziaria	Capacità tecniche e pratiche abituali
Fonte normativa	Stato	Tecnologia
Regole personalizzate	Contratti	Configurazione
Personalizzazione	A basso costo;	Configurazione standard;
Processi	Modulo standard a costi moderati e negoziazione a costi elevati	Scelte dell'utente
Applicazione primaria	Tribunale	Automatizzata, Autoesecuzione

Fonte: J.R. Reidenberg, Lex Informatica, 1998, 566

Osservando la tabella possiamo vedere che sotto il profilo del quadro normativo, con riferimento alla regolamentazione giuridica, alla base di essa abbiamo la Legge, mentre per la Lex Informatica alla base vi sono le Architetture Standard.

[15] J.R. Reidenberg, *Lex Informatica: the formulation of Information Policy Rules through Technology,* 76 Tex. L. Rev 553 (1997-1998)

Per quello che riguarda la giurisdizione, nella regolamentazione giuridica, essa è statale, territoriale mentre con riferimento alla Lex Informatica essa è rappresentata dalla Rete, una rete che scavalca i confini geo-giuridici degli Stati.

Il contenuto della regolamentazione giuridica è costituito da norme prodotte da organi giuridici dello stato e dalle sentenza dei giudici, mentre il contenuto della Lex Informatica consiste nella capacità tecnica del codice di prestabilire quali attività possono essere compiute dagli utenti della rete[16].

Passando alla fonte normativa, per quello che concerne la regolamentazione giuridica, è rappresentata dallo Stato, per la Lex Informatica invece la fonte normativa che va a costituire il codice è il programmatore informatico.

Nella regolamentazione giuridica, attraverso contratti, negozi giuridici, e accordi negoziali si esplica l'autonomia delle regole scelte e decise; mentre nella Lex Informatica, la libertà negoziale delle parti alla quale venivano lasciati i contratti, i negozi giuridici e gli accordi negoziali, viene resa finzione; questo perché essa si riduce a regole tecniche ed a configurazioni preimpostate.

Nella regolamentazione giuridica, il processo di personalizzazione è permesso tramite costi elevati o tramite l'utilizzo a costi più bassi e contenuti di moduli standardizzati, nella Lex Informatica invece viene offerta una vasta gamma di opzioni.

In fine per la regolamentazione giuridica, la forza di legge e data dai tribunali e dalle corti, invece per la Lex Informatica la forza di legge è automatizzata questo per effetto della capacità di elaborazione delle informazioni[17].

Tre importanti caratteristiche, che permettono alla Lex Informatica, di stabilire la politica dell'informazione e la regolamentazione nella società dell'informazione sono che: le regole tecnologiche non si basano su quelle nazionali; si riesce ad avere una facile personalizzazione delle regole ed infine grazie alle capacità di auto applicazione e monitoraggio della conformità le regole tecnologiche possono trarre dei vantaggi.

---

[16] P. MORO, C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Franco Angeli 2017.

[17] P. MORO, C. SARRA, (a cura di) *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Franco Angeli 2017.

6. Impresa e infrastruttura informatica.

L'informazione, nel corso del tempo, per le imprese ha acquisito un'importanza rilevante; è diventata il parametro di riferimento di qualsiasi processo produttivo, economico e finanziario, è diventata il cuore della gestione dei processi di produzione e di analisi della scienza economica[18].

Grazie alla diffusione di internet negli Stati Uniti, si è assistito alla nascita di un nuovo settore economico, la Net Economy, che rappresenta come l'economia che si basa sull'informatica, sia diventata un pilastro del sistema capitalistico globale.

Oggi le imprese se non si dotano di un'infrastruttura informatica, difficilmente possono competere sul mercato con altri e gestire i flussi di dati che provengono dai consumatori attraverso feed back.

Il quadro economico appena descritto si inserisce nel processo di globalizzazione che presenta una veloce evoluzione. La globalizzazione è stata favorita da vari fattori, come esempio la nascita del WTO che ha favorito moltissimo l'interconnessione delle economie nazionali e degli scambi internazionali, ma anche dallo sviluppo di internet che permesso di velocizzare l'instaurazione dei contratti tra le imprese.

La rivoluzione informatica ha influenzato anche il campo giuridico. Nel mondo digitale il diritto tende a seguire di più le merci che viaggiano molto velocemente e di conseguenza l'evoluzione dei metodi di produzione avanza in maniera veloce e tramite un sistema che sembra essere quello del peer-to-peer. In conseguenza di tutto ciò il diritto deve farsi leggero. Di fronte alla globalizzazione questo va a decomporsi, a delocalizzarsi. A differenza dei mercati, le merci, i dati materiali le persone e il diritto inizialmente sono frammentati ma poi si uniscono quando il processo produttivo giunge al termine.

Internet e il mondo digitale, vengono considerati i luoghi in cui assistiamo allo svolgimento dell'attività della maggior parte delle persone. La conseguenza di questo è che su internet avviene il trasferimento di una grande quantità di relazioni. In questo contesto un problema che sorge è quello della protezione dei dati personali, al quale deve essere data una certa precedenza se il diritto vuole continuare a garantire i diritti fondamentali.

---

[18]E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

I dati personali diventano una qualsiasi informazione biografica che fa riferimento ad un soggetto: informazioni economiche, sociali e finanziarie di una persona rientrano a far parte di questa categoria. Tali dati personali rientreranno per sempre nei Big data e quindi fuori dalla possibilità di controllo del soggetto al quale fanno riferimento.

Viene quindi in rilievo la necessità di tutelare i diritti della persona digitale, ovvero il protagonista di questo mondo digitale.

Il mondo all'interno del quale si muove la persona digitale, è il world wide web. Questo ha portato un cambiamento nel modo di vedere il mondo da parte dell'uomo e soprattutto ne ha trasformato usi e costumi. È un ambiente privo di barriere e le regole sembrano essere inesistenti. La conseguenza di ciò è che l'utente si sente libero e non si preoccupa di quali possano essere le conseguenze delle sue azioni.

Tutte le informazioni che l'individuo inserisce nella rete; le tracce digitali lasciate dall'utente durante la navigazione nella rete e dai documenti prodotti dall'interazione con l'ambiente web nel quale si trova, vanno a formare la persona digitale.

Nella vita del mondo reale, la persona si identifica tramite i suoi ricordi, quindi tutto quello che va a definire la sua immagine e la sua biografia, ossia la capacità di auto-riconoscersi ei di andare raggiungere la consapevolezza di qual è il proprio piano di vita. Sul web questa biografia è costituita dai file e dalle informazioni, che la persona produce mentre permane nella rete. Possiamo quindi dire, che nel web, la biografia, sia costituita da una serie di frammenti della propria immagine.

CAPITOLO 2

IL CYBERSPAZIO TRA CYBERLIBERTARIANISMO E CYBERPATERNALISMO

1. La nuova terra di mezzo: il Cyberspazio.

Internet con la sua dinamicità e propulsività, ha rivoluzionato la società portando anche ad un cambiamento del panorama di regolamentazione e comunicazione politica.

Il cyberspazio è una visualizzazione completamente spazializzata di tutte le informazioni presenti in sistemi globali di elaborazione delle informazioni, lungo percorsi forniti da reti di comunicazioni presenti e future, che permette una piena compresenza e interazione tra più utenti, e rende possibile la ricezione e la trasmissione di informazioni attraverso l'intero insieme dei sensi umani, la simulazione di realtà reali e virtuali, la raccolta e il controllo di dati lontani attraverso la telepresenza e una totale integrazione e intercomunicazione con una vasta gamma di prodotti e ambienti intelligenti nello spazio reale[19].

Essa ha la capacità di inglobare ed incanalare, tutta una serie di progetti: realtà virtuale, visualizzazione dei dati, interfacce grafiche, ipergrafica, i multimedia e le reti, verso un obiettivo comune.

Gli oggetti che sono presenti e che si vedono all'interno di questa realtà sono costrutti di dati di pura informazione; essi provengono dal flusso di informazioni che costituiscono l'iniziativa umana nella scienza, nell'arte, nella cultura e nell'economia.

All' interno del cyberspazio, gli enti e le attività che presentano un'alta densità di informazioni presentano una forma, una realtà effettiva ed una identità che possiamo riassumere con una parola: *architettura.* Un'architettura che non può essere vista se non nel cyberspazio; il cyberspazio: ha un'architettura, contiene un'architettura, ed è architettura[20]

Una delle caratteristiche del cyberspazio è che l'uomo comune e l'esperto possono creare, modificare, manipolare e controllare in modo diretto l'informazione.

Esso ci da la possibilità di poter massimizzare i benefici della divisione tra dati, informazione e forma che è resa possibile dalla tecnologia digitale.

---

[19] M. BENEDIKT, *Cyberspace: primi passi nella realtà virtuale.* F. Muzzio, Padova 1993.
[20] M. BENEDIKT, *Cyberspace: primi passi nella realtà virtuale.* F. Muzzio, Padova 1993.

Se pensiamo alla massima giuridica "ubi societas, ibi ius", che afferma che non può esistere una società senza regole, il pensiero di un cyberspazio senza regole potrebbe essere allettante, in realtà si arriverebbe ad uno stato di anarchia invece che di libertà.
Mirta Cavallo nel suo articolo *Internet Governance: l'evoluzione delle teorie sul governo del cyberspazio,* paragona internet al volto di Giano: fonte di enormi benefici- in termini di benefici democratici, sociali, liberalisti, creativi e di diffusione della conoscenza ma che allo stesso tempo possono essere fonte di danno a causa di uno pseudonimo, della mancanza di controllo o supervisione, dell'anonimato, della riduzione della privacy e più sorveglianza e attacchi informatici.
Rousseau, diceva *"l'uomo nasce libero, e dappertutto è in catene"*[21]; ciò significa che per essere liberi e protetti, gli individui devono rinunciare ad una parte della loro libertà riconoscendo la legge di un sistema normativo che si ispira a principi democratici e a diritti fondamentali.
Per la sua natura decentralizzata e priva di confini fa venire meno il concetto di sovranità statale, consente l'arbitraggio e permette di raggirare facilmente qualsiasi intervento statale.

2. Il cyber-libertarismo.

Il libertarismo è quella corrente di pensiero/movimento politico-culturale che pone al centro della sua attenzione il ruolo dell'individuo e la sua libertà di azione all'interno della società capitalista.
M. N. Rothbard, definito il principale teorico del libertarismo postula la necessità di assoggettare alla logica di mercato tutte le funzioni attribuite allo stato e assolutizzare i diritti individuali come naturalmente fondati[22]. Tale corrente di pensiero sostiene la difesa della libertà dell'individuo, oltre che all'interno della società, anche per quello che attiene al diritto e al rispetto della proprietà privata.
Secondo questa corrente di pensiero, l'intervento dello stato è un errore e deve essere il libero mercato ad allocare le risorse in modo efficiente. Da questo ne deriva l'idea che, il potere dello Stato debba essere limitato o in alcuni casi estinto. Ecco che in questo modo,

[21] M. CAVALLO, *Internet governance: the evolution of theories of governing cyberspace.* 14 Maggio 2020 Disponibile in: https://www.cyberlaws.it/en/2020/internet-governance/
[22] Definizione consultabile in: https://www.treccani.it/enciclopedia/libertarismo/

i limiti posti allo stato sarebbero dettati dai diritti individuali, e dovrebbero essere regolati, a tutela dell'individuo, da accordi volontari e dal principio di non aggressione.

Quando parliamo di cyber-libertarismo facciamo riferimento a quell'idea secondo la quale gli individui, nel perseguire i loro interessi e gusti online, dovrebbero essere liberi. L'idea del cyber-libertario è quella del "*vivi e lascia vivere*".
Lo scopo del cyber-libertario è quello di ridurre al minimo la portata della coercizione statale, con riguardo alla risoluzione dei problemi di natura economica e politica, e di cercare invece delle soluzioni volontarie e accordi basati sul mutuo consenso.
Per i cyberlibertari, la vera libertà di internet non consiste nella libertà che lo stato ha di andare a mettere ordine, con lo scopo di migliorare determinate persone o gruppi o per migliorare gli interessi pubblici, ma che sia libertà dall'azione dello stato. Ne consegue che a livello internazionale qualsiasi tentativo di regolamentare il cyberspazio sia fallito
Nell' applicare questa visione, il cyber-libertario non mette in atto una distinzione tra **libertà sociale**: dove ai soggetti dovrebbe essere data libertà di parola, espressione, coscienza e pensiero negli ambienti online e **libertà economica**: dove ai soggetti dovrebbe essere data libertà di contratto, innovazione e scambio negli ambienti online. Le due libertà sono intrecciate, in quanto andare a precludere la libertà in una sfera andrà ad influenzare la libertà nell'altra.
Con riferimento alle prospettive del cyber-libertarismo, vi sono due visioni: **una visione pessimistica** secondo la quale Internet sarà portato sotto il controllo dello Stato e di conseguenza esso andrà ad annullare la libertà online; **una visione ottimistica** secondo la quale gli strumenti e i metodi per evitare la regolamentazione, la censura e il controllo online, ovvero le cosi dette "tecnologie della libertà", prenderanno il sopravvento anche grazie al fatto che la tecnologia si sta evolvendo molto più velocemente rispetto alla capacità che il governo ha di regolarla.

Nei 4 anni compresi tra il 1996 e il 2000, al centro dell'attenzione vi è stato il dibattito sulla regolabilità o meno del cyberspazio, dominato dal dibattito tra cyberlibertario e cyber-paternalista.

La scuola cyberlibertaria ha collegato l'entusiasmo delle forme di vita mediate elettronicamente con le idee libertarie in riferimento alla libertà, alla società e ai mercati[23]. Per i cyberlibertari la libertà di espressione era intrinsecamente protetta nel cyberspazio; non vogliono riconoscere l'intervento dei governi del vecchio mondo; affermano anche che le caratteristiche di progettazione intime ad internet andavano a rendere inutile qualsiasi tipo di intervento statale.

Nel loro seminale, Law and Borders- The Rise of Law in Cyberspace, David Post e David Johnson, hanno espresso, dal punto di vista legale, la classica discussione cyberlibertaria, nella quale si sosteneva che, una regolamentazione che viene fondata sulla sovranità statale tradizionale non può funzionare, così com'è basata su confini fisici.

Notando che il "controllo" emana a livello di singole reti, i due autori hanno proposto che sebbene forme di controllo gerarchico possano essere esercitate su reti specifiche, è improbabile che la gamma aggregata di tali sistemi di regole porti a qualsiasi forme di controllo centralizzato nel Cyberspazio[24].

Per questo la legge del cyberspazio potrebbe essere determinata, per la maggior parte da un libero mercato delle normative, dove gli utenti potrebbero avere la possibilità di scegliere l'insieme di regole che trovano più congeniale.

I cyberlibertari hanno espresso il loro pensiero anche a riguardo di alcuni problemi politici quali: la libertà di parola e sicurezza dei bambini, dove secondo i cyberlibertari si dovrebbe favorire l'emancipazione dei genitori e l'autoregolazione del settore riguardo alla censura; l'informativa sulla privacy e la pubblicità online, riguardo alla quale sostengono che la privacy è una condizione soggettiva e nel regolare la protezione della privacy ci potrebbero essere conseguenze poco desiderate per la libertà di parola e la crescita dei contenuti online e del commercio; la neutralità della rete e regolamentazione delle infrastrutture dove gli operatori di rete dovrebbero essere liberi di possedere, gestire e valutare i propri sistemi e servizi come meglio credono; l'Antitrust dove il potere di mercato e il fallimento del codice sono affrontati dall'evoluzione spontanea dei mercati e dai nuovi ingressi; con riguardo ai diritti di proprietà intellettuale invece alcuni sostengono che siano un'estensione naturale dei tradizionali diritti di proprietà, altri

[23] A. MURRAY, *The Regulatory Edge of the Internet.* International Journal of Law and Information Technology, Vol. 11 No. 1, Oxford University Press 2003.

[24] A. MURRAY, *The Regulatory Edge of the Internet.* International Journal of Law and Information Technology, Vol. 11 No. 1, Oxford University Press 2003.

invece sostengono che nessuno ha diritto di proprietà di creazioni immateriali o che il diritto d'autore sia protezionismo industriale.

3. Cyber-libertarismo e l'eccezionalismo di Internet.

Quando parliamo di cyber-eccezionalismo o eccezionalismo di Internet, facciamo riferimento a soggetti non libertari che si uniscono alle ideologie dei cyber-libertari, perché convinti che Internet debba meritare considerazioni e cure speciali, in quanto convinti che, la storia e la cultura, siano mutate grazie ad Internet.

La prima articolazione dell'Internet eccezionalismo è stata la ***"Dichiarazione dell'indipendenza del cyberspazio"***: "*Governi del mondo industriale, stanchi giganti in carne e ossa, vengo dal Cyberspazio, la nuova casa della Mente. A nome del futuro, vi chiedo del passato di lasciarci soli. Non sei il benvenuto tra noi. Non hai sovranità dove ci riuniamo.*

Non abbiamo un governo eletto, né è probabile che ne avremo uno, quindi mi rivolgo a te senza un'autorità maggiore di quella con cui parla sempre la libertà stessa. Dichiaro che lo spazio sociale globale che stiamo costruendo è naturalmente indipendente dalle tirannie che cerchi di imporci. Non hai il diritto morale di governarci né possiedi alcun metodo di applicazione che abbiamo vere ragioni di temere.

I governi traggono i loro giusti poteri dal consenso dei governati. Non hai né sollecitato né ricevuto il nostro. Non ti abbiamo invitato. Tu non ci conosci, né conosci il nostro mondo. Il cyberspazio non si trova all'interno dei tuoi confini. Non pensare di poterlo costruire, come se fosse un progetto di costruzione pubblica. Non puoi. È un atto della natura e si sviluppa attraverso le nostre azioni collettive.

Non ti sei impegnato nella nostra grande e aggregante conversazione, né hai creato la ricchezza dei nostri mercati. Non conosci la nostra cultura, la nostra etica e i codici non scritti che già forniscono alla nostra società più ordine di quello che potrebbe essere ottenuto da qualsiasi tua imposizione.

Affermi che ci sono problemi tra noi che devi risolvere. Usi questa affermazione come scusa per invadere i nostri distretti. Molti di questi problemi non esistono. Dove ci sono conflitti reali, dove ci sono torti, li identificheremo e li affronteremo con i nostri mezzi. Stiamo formando il nostro contratto sociale. Questo governo sorgerà in base alle condizioni del nostro mondo, non al tuo. Il nostro mondo è diverso."

Oltre a questa dichiarazione, di John Perry Barlow, nel 1994 la Progress & Freedom Foundation grazie al contributo di Esther Dyson, George Gilder, George Keyworth e Alvin Toffler, ha dato vita ad una ***Magna Carta per l'era della conoscenza.*** In questo manifesto gli autori considerano il Cyberspazio la terra della conoscenza e sostengono che la scoperta di questa terra possa essere la vocazione più vera e alta della civiltà. La Terza Ondata ha portato a grandi implicazioni su natura e significato della proprietà, della libertà individuale, della comunità e del mercato. Mano a mano che emerge da vita a nuovi codici di comportamento che smuovono, organismo e istituzioni quali: famiglia, azienda, governo e azione. Viene segnata la morte del paradigma istituzionale ovvero l'organizzazione burocratica.

4. Il pensiero Cyberpaternalista.

Con il termine paternalismo si fa riferimento a tutti quegli atteggiamenti di benevolenza e superiorità, per esempio nel caso delle autorità verso i cittadini. Si pensi ad esempio all'ancien regime dove spesso le autorità erano presentate come il buon padre di famiglia che provvede ai bisogni dei figli senza che però questi potessero partecipare al potere.
Alcuni autori hanno notato che i sostenitori cyberlibertari si basavano su una comprensione semplificata dei fenomeni sociali e politici e che questi avevano una visione di destra dei vari sistemi di regolazione.

Se inizialmente ci si domandava se Internet potesse e dovesse essere regolamentato, ora l'attenzione si sposta sulla questione del come e da chi debba essere governato, con quali valori e nell'interesse di chi; la questione è stata affrontata dai cyberpaternalisti e comunitaristi di rete.
I cyberpaternalisti hanno sviluppato per la prima volta l'idea che Internet non è irregolabile per la sua architettura ma regolato dalla sua architettura.
Con l'operato di Joel Reidenberg, che ha elaborato l'idea di Lex informatica, e poi Lawrence Lessig, che indentifica le quattro forze normative esistenti ed agenti sugli individui che sono: diritto, norma sociali, il mercato e l'architettura, il cyberpaternalismo ha visto la sua età d'oro.
Grazie a questi lavori è stata fissata una nuova prospettiva cyberpaternalista, ovvero che l'architettura della rete non garantisce la libertà individuale. Ciò che vieta o consente l'architettura è il risultato di scelte che non sono solo regole ma anche valori. Lessig

sottolinea: *"siamo così ossessionati dall'dea che libertà significhi libertà di governo che non vediamo nemmeno la regolamentazione di questo nuovo spazio. Nessun pensiero è più pericoloso per il futuro della libertà in cyberspazio rispetto a questa fede nella libertà garantita dal codice. Perché il codice non è fisso, la nostra scelta non è tra regolamento e nessuna regolamentazione. Il codice regola e implementa i valori oppure no. Abilità le libertà, o le disabilità. Protegge la privacy o promuove il monitoraggio. L'unica scelta è se avremo collettivamente un ruolo nella loro scelta o se collettivamente consentiremo ai programmatori di selezionare i nostri valori per noi. Se non lo facciamo, o se non impariamo come, la rilevanza della nostra tradizione costituzionale svanirà."*[25]

L'illusione della libertà si crea all'interno di una sfera altamente regolata dove la regolazione proviene dall'architettura o dal codice. Per i cyberpaternalisti questo rappresenta uno spostamento di potere all'interno del cyberspazio.

Secondo i comunitaristi della rete Andrew Murray, Colin Scott e Roger Brownsword, ci sono diversi difetti nella teoria di Lessig, indentificandoli sono stati in grado di fornire un modello normativo migliore rispetto al Cyberpaternalismo.

Secondo Murray e Scott, una corretta etichettatura deve tenere in considerazione che ogni regolamento ha un direttore, un effettore ed un rilevatore, in più le modalità di regolazione possono essere riformulate come gerarchia, concorrenza, comunità e design.

La classificazione di Murray attinente alle quattro modalità di regolazione nelle due famiglie di modalità socialmente mediate e ambientali, è utile perché mette in evidenza la mancanza di presenza umana, che è anche ciò su cui hanno posto la loro attenzione Scott e Brownsword sotto il punto di vista della responsabilità.

Essa è uno dei principi fondamentali della democrazia requisito indispensabile per la legittimità di una qualsiasi autorità di regolamentazione. Ritenere il codice una modalità di regolamentazione può portare alla privazione degli utenti dell'agenzia morale o della responsabilità dell'uso di internet; essi possono ritenere di essere liberi di fare tutto ciò che è tecnicamente possibile, senza che vi sia la necessità di impegno morale nelle loro attività.

Con questo non si vuole andare a sminuire l'efficacia dell'architettura, ma si deve essere consapevoli del fatto che sia solo uno strumento per far rispettare una regolamentazione.

---

[25] M. CAVALLO, *Internet governance: the evolution of theories of governing cyberspace.* 14 Maggio 2020 Disponibile in: https://www.cyberlaws.it/en/2020/internet-governance/

Lessig sostiene l'idea che gli individui siano punti patetici isolati, osservatori passivi delle regole che li circondano e vincolano. L'errore di questa sua visione è la trascuratezza del ruolo di internet come strumento di comunicazione, riduzione delle distanze e tempi che rafforza però i legami tra persone con gli stessi interessi e le stesse esperienze.
Così facendo però devia da alcune condizioni di forma democratica di Rousseau che sostiene che internet non è solo una rete di reti ma è anche una rete di comunità.

Due degli esponenti del cyberpaternalismo sono Shapiro e Mark Stefik. I loro lavori mettono in luce quali sono i pericoli del controllo attraverso il codice nel tentativo di radunare coloro che si oppongono alla prospettiva di un ulteriore sviluppo della regolamentazione del settore privato all'interno del cyberspazio.[26]
Nel suo lavoro sullo sviluppo di sistemi di gestione dei diritti digitali Mark Stefik ha rappresentato i pericoli che preoccupano i cyberpaternalisti liberali.
Stefik utilizza il termine "*bordo"* proprio come metafora del cambiamento perché sostiene che qualsiasi cosa che non sia familiare o che richieda di effettuare un cambiamento sta ad indicare l'attraversamento di un bordo. Spesso la paura verso il cambiamento spinge il soggetto ad esercitare una resistenza, soprattutto quando incontriamo un limite.
Nell'ambito della nova tecnologia, è proprio quando la società non è pronta ad abbracciare essa, che si verifica questo "respingimento". Stefik è giunto però alla conclusione, che la tecnologia guida il cambiamento, ed è proprio attraversando il limite che si potrà abbracciare il cambiamento portato dalla nuova tecnologia. Grazie al progredire della tecnologia, le persone realizzano che vantaggi e salvaguardie delle nuove tecnologie oltrepassano le loro paure ed è per questo che i confini o "bordi" saranno respinti.
I lavori dei due autori hanno apportato un grande aiuto nella mappatura di questo bordo ovvero di capire dove si trovi questo bordo.
Nella sua opera Shapiro, fa inizialmente una descrizione del potenziale della rete come canale della libertà di parola, come strumento di individuazione e come strumento di

[26] A. MURRAY, *The Regulatory Edge of the Internet.* International Journal of Law and Information Technology, Vol. 11 No. 1, Oxford University Press 2003.

disintermediazione; in questo modo, mette il lettore, davanti ad un futuro in cui il controllo è offerto agli individui. Grazie al potere di pubblicare, gestire e filtrare dati su una scala che prima era inimmaginabile permetterà ad individui e comunità di sviluppare standard e strutture di regolamentazione libere dalle odierne istituzioni.

Dobbiamo però dire che in un secondo momento Shapiro va a rompere le speranze libertarie. Pone a confronto le tecniche di regolamentazione più efficienti ed efficaci utilizzate da Microsoft e altri partner con i tentativi da parte dei governi di regolamentare le nostre azioni nel cyberspazio. La sezione dedicata alla Resistenza rappresenta il fulcro dell'analisi fatta da Shapiro. Tale analisi però cade se non accettiamo le sue credenze cyberpaternaliste.

Negli ultimi due atti si sofferma nell'analizzare il rischio del "sovrasterzo", questo è il rischio che gli individui, inesperti nelle nuove tecnologie di spingere oltre la nuova libertà trovata e subire conseguenze inaspettate. Degli esempi di sovrasterzo possono essere: l'evitamento selettivo delle informazioni attraverso l'uso di strumenti di filtraggio e la perdita di comunità a causa dell'isolamento e della facilità di uscita.

5. Come viene regolato internet tra cyberlibertarianism e cyberpaternalism.

Il diritto, secondo i sostenitori dell'approccio normocentrico, continua a disciplinare le attività digitali di ogni cybernatura.

In internet, alcune tra le tante difficoltà, risalgono alla definizione delle relazioni tra spazio reale e virtuale e nello stabilire come predisporre un diritto della rete; infatti, non può essere ancorato ad uno spazio territoriale ma serve individuare delle linee di confine logiche.

I giuristi di diritto positivo ritengono che qualsiasi attività che ha luogo in rete viene disciplinata da una norma alla quale si deve prestare attenzione, in quanto la rete è un luogo profondamente concreto e capace di accogliere nel suo seno, nel bene e nel male, le più umane esigenze[27].

Il cyberspazio è uno spazio del mondo reale, perché da quest'ultimo può essere regolato ma specialmente perché i suoi utenti vivono nella realtà fisica. L'unicità del paradigma

[27] E. MAESTRI, *Lex Informatica e soft law. Le architetture normative del cyberspazio,* settembre 2017.

cyberspace as place sta nella interazione che si realizza tra il potere normativo e la progettazione tecnica.

In contrapposizione alla prospettiva del "il diritto doma il code", la corrente cyberlibertaria, ha reclamato la natura libertaria della rete, andandola a qualificare come un unico spazio virtuale che doveva restare fuori da qualsiasi tipo di regolamentazione.

A causa dell'anonimità e della multi-giurisdizionalità che caratterizzano il cyberspazio, le condotte sfuggono al controllo del governo; è la natura stessa dello spazio digitale a rendere irregolamentabile il comportamento.

Secondo i sostenitori del cyberlibertarianism, la governance del cyberspazio ha origine dal basso (*bottom up)* le regole sono dettate dai singoli utenti che sono legittimati dall'utilizzo della rete.

Da un lato però, presupporre che l'architettura, possa essere fissata *by default* e che il governo possa essere incapace di ricorrere a misure efficaci che possano modificarla, renderebbe sbagliata la credenza sull'architettura ontologica e normativa del cyberspazio.

Si deve però ammettere che la *self-regulation approach* del cyberspazio prende in considerazione una questione reale, ovvero che la fonte primaria in rete resta un processo decentralizzato di adozione volontaria di standard tecnici da parte di operatori in rete, piattaforme web e comunità degli utenti[28].

È proprio l'esistenza di diverse sotto-comunità di utenti, che comporta l'eterogeneità delle regole applicabili.

In accordo con quanto elaborato da Lessig, si ritiene che l'architettura del cyberspazio sia fissata in funzione del design.

L'architettura del cyberspazio è neutrale. Utilizzare l'architettura per regolare la condotta comporta la disarticolazione dei principi stessi sui quali si fondano gli ordinamenti giuridici costituzionali.

Se pensiamo alla proprietà intellettuale digitale, il code risulta sovrainclusivo rispetto alla normativa giuridica. Essa permette una implementazione architettonica del code che sia tale da favorire i detentori di grandi percentuali di proprietà intellettuale.

[28] E. MAESTRI, *Lex Informatica e soft law. Le architetture normative del cyberspazio,* settembre 2017.

Nell'ambito del copyright, si è verificato un restringimento dei margini di libertà riguardanti la scelte individuali.

La società post-internet determina un accrescimento della normativa sul copyright, come sostegno delle grandi imprese che producono contenuti digitali.

Il diritto interagisce con il code, andando a sua volta ad impedire che, le protezioni tecnologiche e la produzione di tecnologie finalizzate ad eludere tali protezioni, vengano aggirate.

L'architettura diventa quindi, un vincolo molto forte per l'individuo e risulta molto invasiva delle sue capacità di azione: la proprietà digitale diventa proprietà mimetica dell'architettura e pone controlli e regole, influendo su mercati e legge[29].

6. Internet quale forma di commons.

Internet è considerato un bene in comune e gratuito, ovvero una forma di commons.

Una risorsa alla quale chiunque ha diritto di accedere senza dover chiedere il permesso per accedervi.

Le norme, l'architettura, il Web 1.0, il Web 2.0, tutto questo continua a restituire Internet come una forma di commons.

Sono tre gli aspetti principali di questo bene comune:

1. Il già citato codice, ovvero un commons di software;
2. Il commons di conoscenza, dove lo scambio di idee e di informazioni avviene liberamente;
3. Il commons di innovazione, cioè permette e chiunque di innovare e di costruire la piattaforma del network;

Un codice libero costituisce un commons di conoscenze, reso possibile dalla natura dell'informazione[30].

[29] E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

[30] E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

Inizialmente nel World Wild Web, la maggior parte dell'apprendimento si basava sul copiare una pagina e modificarla secondo la volontà del programmatore. Il common invece è una risorsa decentralizzata. I protocolli della rete spingono ad innovare.

Si potrebbe pensare ad internet non come un sistema costruito a rete ma come un sistema a strati:

1. il primo strato è quello fisico, rappresentato dal computer attraverso il quale passa la comunicazione;
2. il secondo strato è quello logico, che è costituito dal codice;
3. il terzo strato contiene ciò che si trasmette;

I tre strati lavorano assieme ma si alternano tra libertà e controllo. Il primo strato, quello fisico ed il terzo strato quello di contenuto sono controllati.

La necessità di regolare Internet ha portato alla creazione di un consistente gruppo di norme e ha contribuito allo sviluppo di una serie di principi che si sono diffusi ben oltre il loro ambito originario.

I prodotti diffusi sul web aumentavano, gli utenti si diversificavano e man mano che cresceva la compatibilità tra piattaforme, le aziende esercitavano un controllo sempre maggiore sulla modalità di utilizzazione di vari prodotti[31].

Tutto questo fece in modo che il code si sviluppasse in modi diversi e sempre più legati alla proprietà.

[31] E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

CAPITOLO 3

CRIMINALITÀ ORGANIZZATA INFORMATICA

1. Criminalità informatica: nozione, strumenti di contrasto e il problema della territorialità.

Ad oggi, nonostante compaia in fonti europee e sovrannazionali, la criminalità informatica, non consiste in una categoria definita giuridicamente.

Nel tempo da un lato è sorta la necessità di punire fatti nuovi, commessi tramite le tecnologie e la rete, lesivi dei beni giuridici tradizionali e dall'altro sono affiorate nuovi interessi degni di protezione penale.

Non si ha nemmeno una definizione riconosciuta a livello internazionale di computer crime o cybercrime.

Sul piano empirico, essa abbraccia una molteplicità di comportamento lesivi di interessi penalmente rilevanti, riconducibili ai reati informatici, introdotti in molti ordinamenti nazionali[32]; sul piano fenomenico, dopo l'esplosione di Internet e con il passaggio dalla dimensione privata/individuale del computer a quella pubblica/collettiva dei sistemi che sono basati sull'interconnettività globale.

Parte della dottrina americana sostiene che il cybercrime presenti tre sottocategorie:

- Reati dove, l'obiettivo dell'attività criminale, sono il computer o il sistema informatico;
- Reati dove gli strumenti per preparare e commettere il reato, sono rappresentati dal computer e da Internet
- Reato nei quali la rete ed i sistemi informatici costituiscono un aspetto incidentale nel commettere l'illecito;

Viene condivisa la tesi secondo la quale la criminalità informatica includa sia fattispecie legali che sono costruite con elementi di tipizzazione connessi a procedimenti di automazione di dati o informazioni, ovvero legate a oggetti o attività di carattere tecnologico, sia quelle fattispecie incriminatrici comuni che anche se non presentano

[32] A. M. MAUGERI (a cura di), *Stati Generali della Lotta alle Mafie, Tavolo XV- "Mafie e Europa",* in Diritto Penale contemporaneo, 2019

elementi tipici di carattere tecnologico, possono essere applicati a fatti connessi tramite la tecnologia, il cyberspazio e la rete.
Qui viene in rilievo anche la distinzione tra i reati cibernetici in senso stretto, dove l'elemento tecnologico è caratterizzato dalla connessione in rete o dalla fruibilità del cyberspace; al contrario quelli in senso ampio vanno a costituire la modalità o possibilità attraverso la quale si realizzano i reati.

Nel contrasto alla criminalità informatica uno degli strumenti più rilevanti è la Convenzione sulla criminalità informatica di Budapest del 2001.
Essa all'Articolo 13, ci dice che: ogni parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie affinché i reati previsti in applicazione degli articoli da 2 a 11 possano essere puniti con sanzioni effettive, proporzionate e dissuasive, che includano la provazione della libertà. Ogni parte deve assicurarsi che le persone giuridiche ritenute responsabili, in base all'articolo 12, siano assoggettate a sanzioni penali o non penali effettive, proporzionate e dissuasive o ad altre misure, incluse sanzioni pecuniarie[33].
In Italia tale convenzione è stata ratificata con la l. 18 marzo 2008, n. 48, che è anche intervenuta in 4 macrosettori del nostro ordinamento: nel Codice penale, nel Codice di procedura penale, nel D.lgs. 30 giugno 2003, n. 196 ovvero il c. d. Codice della Privacy e nel D.lgs. 8 giugno 2001, n. 231.
Un segnale rilevante della lotta contro la criminalità informatica è rappresentato dalla direttiva europea 2013/40/UE. Essa evidenzia anche lo stretto rapporto che vi è con la criminalità organizzata.
Gli attacchi causati ai sistemi di informazione, sono in continua crescita ed evoluzione; questo comporta una minaccia per la costruzione di una società dell'informazione sicura e di uno spazio di sicurezza, libertà e giustizia.
Proprio per questo l'Unione Europea ritiene sia necessario, soprattutto, prevedere sanzioni più severe nel momento in cui un attacco a questi sistemi provenga da un'organizzazione criminale.

[33] *Convenzione del Consiglio d'Europa sulla criminalità informatica.* Budapest 23 novembre 2001. Osservatorio permanente sulla criminalità organizzata.

Inoltre, gli Stati membri, dovrebbero rendere migliore la collaborazione internazionale relativamente alla sicurezza dei sistemi dell'informazione, delle reti informatiche e dei dati informatici.

Il problema principale delle norme giuridiche, riguardo alla cogenza, risiede proprio nel fatto che la rete si colloca oltre il raggio d'azione delle leggi statali. Essendo così risulta difficile determinare se e come possa essere possibile perseguire chi ha agito in un paese diverso da quello in cui la violazione di legge è stata messa in atto.
Ecco che diventa necessario, avere oltre che le leggi statali anche delle convenzioni internazionali.
Internet e i software vengono regolati anche tramite accordi conclusi in regime di soft law. La tendenza è quella di rifiutare il paternalismo legislativo, che è destinato a rispettare la libertà delle reti e a salvaguardare i diritti degli utenti, per affidarsi ad una logica di mercato, a forme di soft law imposte sugli utenti dai tecnici informatici.
Il confidare negli algoritmi, nel codice binario, ne determina una presenza sempre più pervasiva che sembra non conoscere confini[34].
Il code razionalizza le procedure, calcola variabili difficili da governare, ma non può considerare tutti i caratteri imprevedibili degli accadimenti, cosa che invece un giudice può fare. La macchina non può sostituire l'uomo, quando si devono salvaguardare i diritti e punire le violazioni di legge[35].
Ricordando il confronto tra Regolamentazione Giuridica e Lex informatica messo in luce da Reidenberg; uno degli elementi al quale possiamo fare riferimento e che spesso, nel caso dei crimini informatici risulta essere un aspetto che crea ostilità, è quello legato alla **giurisdizione**, che nell'ambito della regolamentazione giuridica è territoriale, ovvero si basa su confini fisici, mentre per la Lex informatica è la rete, priva di confini fisici.
La minaccia criminale, nel mondo virtuale non è assimilabile a quella tradizionale, strettamente radicata sul territorio e quindi localizzata, ma assume una connotazione

[34] S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli.* Edizioni Laterza, 2014.
[35] E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

transnazionale. La caratteristica peculiare è infatti la distanza tra i cybercriminal e le loro vittime potenziali[36].

Nel diritto penale, il principio di territorialità, è uno dei principi che delimita la sfera di applicazione territoriale della normativa penalistica.[37]

Nel nostro ordinamento giuridico tale principio, viene espresso all'articolo 6 c.p. *"Reati commessi nel territorio dello stato"*. Il principio dà la possibilità di punire una determinata condotta purché questa sia stata posta in essere all'interno del territorio italiano, a prescindere che il soggetto attivo del reato sia un cittadino italiano o straniero o apolide.

Nell'ambito di internet e del cyberspazio però sorgono delle criticità dovute al fatto che, per esempio grazie alla globalizzazione vi sia stato un passaggio da territorialità a spazialità; una delle caratteristiche principali di internet è la delocalizzazione, che porta ad una moltiplicazione dell'azione nello spazio. Tutto quello che ha luogo nella rete, a differenza di quello che può avvenire all'interno di un territorio fisico come lo Stato, non conosce confini territoriali, geografici e giuridici e subisce dei condizionamenti da quello che possiamo definire ecentricità delle comunicazioni elettroniche.

Quando un reato ha luogo all'interno della rete o viene commesso avvalendosi di mezzi informatici e telematici, come nel caso dei crimini informatici, risulta non sempre facile individuare il luogo del reato; questo perché raramente il luogo del reato coincide con un territorio fisicamente identificabile, proprio perché la condotta avviene in uno spazio senza confini.

La giurisdizione italiana si può applicare quando per esempio, le informazioni che vanno a costituire oggetto del reato, benché siano state immesse in rete all'estero, siano passate attraverso server collocati all'interno dello stato italiano.

In base al principio di ubiquità, il giudice italiano può riconoscere il fatto come costituente reato sia nel caso in cui la condotta si sia verificata all'interno dello Stato italiano, sia se il crimine, che ha avuto inizio al di fuori dei confini statali, si sia concluso con un evento realizzato in Italia.

---

[36] G. ILARDA e G. MARULLO (a cura di) *Cybercrime: Conferenza Internazionale. La convenzione del Consiglio d'Europa sulla Criminalità Informatica.* Milano, GIUFFRÈ EDITORE 2004.

[37] Consultabile in: https://www.diritto.it/il-principio-di-territorialità-in-diritto-penale

2. Le difficoltà difronte alle quali si trova il diritto in merito al crimine informatico.

Negli anni 60 erano principalmente i criminologi a studiare e affrontare il fenomeno della criminalità informatica; i giuristi hanno cominciato ad occuparsi di criminalità informatica successivamente, ovvero quando si sono cominciate a riscontrare difficoltà nell'inquadramento dell'illecito informatico.

L'articolo 615 ter c.p. affronta uno dei più grandi problemi del diritto penale dell'informatica. Sono venute alla luce parecchie perplessità in sede dottrinale da parte di molti governi nella penalizzazione di tale comportamento. Questo perché in passato i legislatori erano influenzati dalla considerazione secondo cui la penetrazione in un sistema senza intenzioni cattive, con l'intenzione cioè di ottenere soltanto delle informazioni, sia pur facendo ricorso a mezzi illegittimi non costituirebbe un fatto degno di attenzione da parte del sistema penale[38]. L'opinione pubblica in merito a ciò si era dimostrata indulgente nei confronti degli hacking e proprio questa opinione ha ritardato e reso difficile la penalizzazione del comportamento in questione.

Si riscontrano nel "rapporto" tra diritto penale dell'informazione e reati informatici alcune problematiche, criticità come: la necessità di una valutazione sistematica, in quanto la categoria dei reati informatici non va ad individuare un ambito di tutela che abbia contenuti omogenei; si presenta anche insufficiente la bipartizione che vede da un lato le fattispecie che prevedono nuovi mezzi o modalità d'aggressione ai beni giuridici tradizionali e dall'altro le fattispecie che offendono beni giuridici nuovi.

Un'altra difficoltà difronte alla quale si trova il diritto è quella dello sviluppo delle comunicazioni per via informatica e telematica, collegato alla diffusione globale di Internet che ha portato alla luce nuove possibilità e modalità di aggressione dei beni giuridici tradizionali, vicino a nuovi interessi meritevoli di tutela penale. Per questi risulta, inoltre, ancora incerta la riconducibilità alla disciplina penale vigente o la necessità di prevedere delle nuove previsioni sanzionatorie. Difronte a questa evoluzione del diritto penale dell'informatica nell'epoca di internet si dimostra l'utilità di risalire ai diversi tipi di rapporto costitutivi dei fatti tipizzati dalle singole disposizioni penali per giungere ad una corretta risoluzione dei problemi di classificazione e collocazione

[38] L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet.* Dipartimento di scienze giuridiche Università di Trento. CEDAM 2004.

sistematica, non che di valutazione critica circa le necessità di nuove previsioni incriminatrici[39].

Riprendendo nuovamente quanto riportato da Reidenberg, nella sua teoria, emerge, che la fonte normativa nella regolamentazione giuridica dipende dallo Stato, ovvero dalle sue istituzioni destinate all'emanazione di norme e leggi. Per la Lex informatica invece, la fonte normativa è rappresentata dal programmatore informatico, che va a costituire il codice. Con l'avvento di nuove tecnologie, con la continua evoluzione di Internet e dell'informatica, si sono verificati, un cambiamento ed un'evoluzione in alcune forme criminali. Da questo possiamo notare come la tecnologia, con il suo progredire possa influire sulla necessità dello Stato, di adeguare la normativa già vigente:

a) o portandolo a modificare la normativa già in vigore nel nostro ordinamento;
b) o portandolo a emanare nuove norme per contrastare queste nuove forme di criminalità;

3. I rapporti tra "Crimine organizzato" e "Crimine informatico"

Quello che sembra costituire il minimo comune denominatore della criminalità organizzata è rappresentata da un'organizzazione strutturata di persone, che collaborano per un periodo di tempo prolungato, finalizzata all'arricchimento, sia personale che dell'organizzazione, attraverso la commissione di reati[40].

Le connessioni tra le due realtà criminali comprendono una variegata fenomenologia di attività criminali. Il cybercrime non è più dominato da hackers. L'evoluzione della digital economy, del deepweb e del darknet ha portato ad una trasformazione dello scenario. Se pensiamo alla rete ad oggi conosciuta dagli utenti, possiamo immaginarla come un grande iceberg, dove la parte sommersa rappresenta il deepweb, ovvero uno spazio pieno di risorse informative del WWB che i classici motori di ricerca non indicano o segnalano, ed al quale si può accedere solo mediante software o browsers specifici. All'interno di essi gli utenti possono svolgere molteplici attività, legali o illegali, tra cui ad esempio tecniche di dissimulazione dell'ip-address.

---

[39] L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet.* Dipartimento di scienze giuridiche Università di Trento. CEDAM 2004.
[40] A. M. MAUGERI (a cura di), *Stati Generali della Lotta alle Mafie, Tavolo XV- "Mafie e Europa",* in Diritto Penale contemporaneo, 2019.

La comunicazione tra gli esponenti di gruppi criminali o anche fra gli stessi gruppi criminali, attraverso scambi di informazioni nel deep web o nelle darknet, l'accessibilità a tools, softwares e browsers per operazioni illegali, tutte quelle attività di monitoraggio dei social media e social network, vengono considerate attività normali ma che possono costituire attività di preparazione alla realizzazione di illeciti di rilevanza penale.

Soprattutto nel deep web, ed ancora più precisamente, le darknet e i blackmarkets costituiscono i "luoghi" principali di aggregazione nei quali l'accesso al gruppo e l'attendibilità di chi partecipa sono verificati e verificabili e le vie di fuga sono sicure e anonime.

In questi cyberspazi avviene l'incontro tra domanda e offerta, di attività illegali tra le quali: traffico di armi, traffico di organi, riciclaggio e cyberlaundering, hacking, traffico di esseri umani, pedopornografia.

Tutto questo è agevolato dal fatto che nel deepweb, viene assicurato l'anonimato, facile accessibilità e protezione anche grazie all'utilizzo del bitcoin, una moneta-valuta virtuale, ed a fattori come la crescita che questo "ambiente", privo di confini, sta avendo.

Appare evidente come il collegamento fra crimine organizzato e crimine informatico sia caratterizzato da elementi strutturali complessi e in continuo cambiamento, soprattutto a causa del progresso tecnologico[41].

I rapporti che si sono creati tra crimine organizzato e crimine informatico vanno interpretati tenendo presente alcune prospettive quali: a) la criminalità organizzata c.d. tradizionale si avvale di Internet con lo scopo di commettere dei reati o mettere in atto attività preparatorie con il fine di investire o occultare proventi di origine delittuosa o le tracce del reato; b) la criminalità organizzata può avvalersi di servizi che vengono offerti da professionisti per compiere azioni quali la compravendita di identità digitali o nuovi documenti di identità, acquisizione di informazioni attraverso accessi illeciti a sistemi informatici, danneggiamento di sistemi informatici, o di dati e informazioni in essi archiviati; c) il **COC** (cyber-organized-crime), ovvero il crimine informatico organizzato: gruppi criminali che operano nel cyberspace e commettono reati informatici in senso lato oppure offrono i loro servizi a singoli o ad altri gruppi criminali per la commissioni di altri reati. Tramite la tecnologia questi gruppi si assicurano la sopravvivenza realizzando

[41] A. M. MAUGERI (a cura di), *Stati Generali della Lotta alle Mafie, Tavolo XV- "Mafie e Europa",* in Diritto Penale contemporaneo, 2019.

frodi o reati economici, oppure sfruttano le risorse del gioco d'azzardo online, e da un lato offrono le loro professionalità.

Questo tipo di nuova generazione nasce proprio per essere attivo nel cyberspazio, un ambiente privo di confini, globalizzato e immateriale dove il reato assume una forma transnazionale.

4. Il caso JAMMJAMM.

Uno degli ambiti in cui la criminalità organizzata svolge attività illecite è quello del gioco d'azzardo.

Grazie ad un'indagine condotta dalla Direzione distrettuale antimafia del Tribunale di Salerno chiamata operazione JamJam ha messo in luce l'esistenza di un sodalizio criminale che operava sul territorio italiano, in particolar modo il Basilicata, Campania e Calabria, e con estensioni a livello internazionale i Canada, Regno Unito, Malta e Montenegro, dedicato al gioco d'azzardo online con l'utilizzo di piattaforme illegali di siti web esteri abusivamente attive. Tutto in assenza dell'autorizzazione da parte dell'Amministrazione Autonoma dei Monopoli di Stato.

I siti web erano stati alterati in modo tale da non permettere al giocatore di effettuare vincite apprezzabili. Tali piattaforme illecite venivano "ospitate" da gestori di esercizi commerciali.

L'organizzazione criminale è riconducibile alla famiglia dei Contaldo di Pagani. I principali promotori di questa attività illecita sono stati, Contaldo Antonio unitamente ai fratelli, figli, e familiari che gestivano svariate piattaforme e canali online per la raccolta delle scommesse clandestine e del poker su Internet, creandone anche di proprie.[42]

Contaldi si è avvalso anche di collaborazioni con altre organizzazioni che operavano sul territorio nazionale quali, i fratelli Tancredi di Potenza e di soggetti vicini alla 'Ndrangheta Calabrese. Per sviluppare ed imporre le piattaforme che creava si avvaleva anche dell'aiuto persone affiliate a clan camorristici, nonché a pluripregiudicati con esperienze nel settore dei giochi online.

[42] Si veda https://www.zerottonove.it/operazione-jamm-jamm/

Per portare a compimento i fini illeciti dell'organizzazione avevano il supporto da vari esercenti commerciali che ospitavano le piattaforme illecite di gioco ma anche di raccolta delle scommesse. I profitti che venivano raccolti erano utilizzati per investimenti commerciali.

Su delega della Procura della Repubblica di Salerno, la Direzione distrettuale Antimafia i militari del Comando Provinciale della Guardia di Finanza di Salerno hanno disposto 18 ordinanze di custodia cautelare che sono state disposte dall' Ufficio del G.I.P. del Tribunale di Salerno, nei confronti di un sodalizio criminale con sede operativa nell'agro nocerino sarnese.

Nell'ambito dell'operazioni sono stati posti sotto sequestro ed oscurati 11 siti internet illegali, avvalendosi degli specialisti del Nucleo speciale frodi tecnologiche della guardia di finanza, con sede a Roma. Inoltre, sono state poste sotto sequestro 23 attività commerciali e beni mobili registrati[43].

Le indagini hanno portato alla luce diversi capi di imputazione a carico degli indagati, tra cui 57 sono stati ritenuti associati all'attività criminale. Tra le varie imputazioni si parla di rivelazione di segreto d'ufficio da parte di tre agenti di alcuni corpi di polizia.

5. L'operazione internazionale "FONTANA-ALMABAHIA"

L'operazione FONTANA-ALMABAHIA ha coinvolto 106 soggetti, per la maggior parte italiani residenti a Tenerife, i quali erano in contatto con alcune associazioni mafiose.

Le vittime italiane ed europee venivano tramite tattiche come la truffa del Ceo oppure tattiche quali: sim swapping dove ci si appropria del numero di telefono delle vittime violandone i servizi online; il phishing che consiste nell'inviare mail apparentemente proveniente da fonte affidabile (banca), con lo scopo di prelevare dati riservati e prosciugare i conti correnti delle vittime; il vishing simile ai precedenti, dove i truffatori attraverso la rete effettuano telefonate che sembrano provenire da un call center in realtà le effettuano loro stessi. In questo modo si ottengono credenziali bancarie attraverso gli account delle vittime, si eseguono bonifici destinati ai money mules che provvedono in

[43] Si veda https://www.zerottonove.it/operazione-jamm-jamm/

cambio di una percentuale sui guadagni ad aprire conti correnti ad hoc attraverso cui transita il denaro prima di arrivare alle casse dei vertici della rete[44].
Tramite l'aiuto di informatici esperti hanno svuotato decine di conti correnti e riciclato i soldi guadagnati in due modi: investendoli in criptovalute e in parte finanziando la produzione e il traffico di stupefacenti, compravendita di armi e lo sfruttamento sessuale.

La polizia spagnola in un comunicato stampa scrive che è stato un duro colpo per la mafia e racconta dei continui viaggi di un esponente della camorra a Tenerife.
La polizia postale e la procura di bari, ci dico però che le indagini nel nostro paese non hanno al momento sufficienti prove che i soggetti coinvolti nell'operazione siano affiliate a un'organizzazione mafiosa in Italia.
Ivano Gabrielli, vicedirettore della Polizia postale che ha condotto le indagini in collaborazione con l'Europol ed Eurojust, sostiene che questi sono criminali che avevano contatti con la camorra, la 'ndrangheta e la mafia romana, però in Italia non risultano indagati per associazione mafiosa.[45]
In una delle ultime relazioni della Direzione Investigativa Antimafia (DIA), questa mette in evidenza che vi è una capacità della mafia, di cogliere le opportunità che vengono offerte dalla globalizzazione, la quale si rinviene nel ricorso all'utilizzo di criptovalute come Bitcoin.

6. Il COC-Cyber Organized Crime e sue caratteristiche.

La dottrina, vista la complessità raggiunta dalle attività criminali nel cyberspace, ha cominciato a parlare di cybercrime organizzato.
Dai risultati di alcuni reports di ricerca, si è giunti all'identificazione di tre principali gruppi criminali e sei sottotipi, giungendo alla conclusione che l'80% dei reati informatici può definirsi organizzato, in senso lato.

[44] R. RIJTANO, *Truffe online, cyber riciclaggio e narcotraffico: la criminalità organizzata si reinventa.* Lavialibera, 23 settembre 202, https://lavialibera.it/it-schede-690-truffe_online_cyber_riciclaggio_e_narcotraffico_la_criminalita_organizzata_si_reinventa
[45] R. RIJTANO, *Truffe online, cyber riciclaggio e narcotraffico: la criminalità organizzata si reinventa.* Lavialibera, 23 settembre 202, https://lavialibera.it/it-schede-690-truffe_online_cyber_riciclaggio_e_narcotraffico_la_criminalita_organizzata_si_reinventa

Tra i vari gruppi criminali quelli più conosciuti sono: **DrinkOrDie**, dove venivano riprodotti e distribuiti softwares, games e movies in Internet. Era un gruppo molto sofisticato a livello tecnologico e ben organizzato con competenze nell'ambito della sicurezza, programmazione e comunicazione via Internet. I paesi coinvolti sono stati UK, Australia, Finlandia, Norvegia, Svezia e U.S.A.; **Dark Market**, forniva infrastrutture per mettere in contatto compratori e venditori di carte di credito e identità digitali per poter accedere a servizi bancari o finanziari. Il recupero dei dati attraverso diversi metodi illegali come, ad esempio, un accesso abusivo ai sistemi informatici skimming o phishing attacks. Per accedervi i membri coinvolti dovevano essere in possesso di dati e informazioni reali da poter utilizzare, la protezione era di sicurezza elevata, i paesi coinvolti erano UK, Canada, U.S.A, Russia, Turchia, Germania e Francia; **DNSChanger**, gruppo specializzato nel controllo di DNS changer malware, che rendeva possibile il controllo di DNS servers; il malware era diffusa attraverso i social engineering e permetteva di effettuare frodi informatiche tramite il redirecting degli utenti, tramite il controllo su server che ospitavano fake websites promuovendo addirittura prodotti contraffatti e molto pericolosi.
La finalità che accomunava queste organizzazioni era quella di ottenere un lucro o profitto.

Le varie reti criminali che operano nel cyberspace o tramite il cyberspace non sono collegate tra loro. Ciascuna ha le proprie funzioni e ruoli.
Spesso hanno dei coore memebers che sono adibiti al coordinamento dell'attività ed il network degli enablers, offrendo e fornendo servizi e tecniche per commettere reati. Come ultima figura di queste organizzazioni ci sono i money mules che hanno il compito di trasferire i proventi illeciti.
Il cyber organized crime ha un certo interscambio organizzativo flessibile e fluido dove si avvale di soggetti esterni che operano fuori dal cyberspace per compiere attività criminali, ad esempio, manager di istituti bancari o dipendenti infedeli reclutati per operazioni tipo installazioni o attivazione su device o server.
Grazie all'operazione EMMA (European Money Mules Action) condotta dal 22 al 26 febbraio, dal servizio di Polizia postale, in collaborazione con diverse Forze di polizia

europee, e con la collaborazione di Europol-European Cybercrime Center e il supporto di Eurojust e della Federazione bancaria europea, sono stati individuati 700 money mules[46]. Questi Money mules, ovvero i primi destinatari dei soldi ricavati dalle frodi informatiche o dalle campagne di phishing, mettevano a disposizione la loro identità con il fine di aprire conti correnti o carte di credito sui quali, le somme frodate venivano accreditate, ad esempio attraverso attacchi ai sistemi di home-banking. Tali somme una volta ottenute vengono divise tra i money mules che ne trattengono una parte ed il restante viene trasferito su conti che fanno capo alle organizzazioni criminali anche di paesi diversi. Grazie al supporto di oltre 50 istituti bancari, sono stati individuati oltre le 800 transazioni bancarie fraudolente, è stato sequestrato denaro per più di un milione e mezzo di euro.

Una classificazione del cyber organized crime, si può ottenere considerando la natura o la caratteristica dell'attività criminale e possono essere suddivise in tre categorie:

- reati commessi al fine di ottenere profitti economici: eseguiti attraverso attacchi a sistemi bancari, sistemi informatici o singoli utenti, traffico d'armi, traffico d'organi e stupefacenti;
- servizi che vengono offerti a terzi anche in deepweb e darknet;
- offerta di servizi ad alto contenuto tecnologico;

Vi è anche una seconda classificazione che si può basare principalmente sul ruolo che la tecnologia ha, combinata alla finalità che il gruppo criminale ha:

- gruppi che utilizzano le ICTs, che opera solo nel mondo reale
- cyber organized crime che opera esclusivamente nel cyberspazio e online;
- gruppi organizzati da idee o propositi politici che utilizzano le tecnologie per supportare o facilitare le loro attività illegali[47].

[46] Si veda https://www.interno.gov.it/it/notizie/cybercrime-operazione-emma-contro-i-money-mules-81-arresti

[47] A. M. MAUGERI (a cura di), *Stati Generali della Lotta alle Mafie, Tavolo XV- "Mafie e Europa",* in Diritto Penale contemporaneo, 2019.

7. Strumenti penalistici di tutela, inerenti alla tecnologia e alla rete quando queste costituiscono il mezzo per la commissione del reato.

I reati informatici sono stati introdotti nel Codice Penale dalla legge 547/1993 e limitati ai soli casi di particolare complessità e a quelli commessi attraverso l'impiego di tecnologia informatica o telematica.

Si intendono in particolare i seguenti fenomeni illeciti: DIALER, FURTO DI IDENTITÀ SEMPLICE, VIOLAZIONE ACCOUNT, ACCESSO EMAIL, ALTRO ACCESSO ABUSIVO A SISTEMI INFORMATICI, TRUFFA E-BAY O SU ALTRE PIATTAFORME DI E-COMMERCE, BONIFICO/RICARICA DISCONOSCIUTA (PHISHING), RICICLAGGIO ELETTRONICO PROVENTI ILLECITI (CYBERLAUNDERING), CARTE DI CREDITO[48].

Il Codice Penale Italiano, in merito ai precedenti illeciti, stabilisce:

- *Art 615 ter, c. 1Accesso abusivo ad un sistema informatico o telematico*: 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, è punito con la reclusione fino a tre anni[49].
- *Art 615 quater, detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*: chiunque al fine di procurare a se o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo è punito con la reclusione sino a due anni e con la multa sino a 5.164 euro[50].
- *Art 640 ter Frode Informatica*: Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto

[48] Si veda https://www.procura.milano.giustizia.it/reati-informatici.html
[49] E. DOLCINI-G.L. GATTA, *Codice Penale e norme complementari.* Edizione aggiornata al 22 agosto 2019, GIUFFRÈ FRANCIS LEFEBVRE.
[50] E. DOLCINI-G.L. GATTA, *Codice Penale e norme complementari.* Edizione aggiornata al 22 agosto 2019, GIUFFRÈ FRANCIS LEFEBVRE.

profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 a euro 1.032[51].

Approfondendo la connessione tra criminalità informatica e criminalità organizzata tra cui il fenomeno mafioso si ricorda, *l'articolo 416 bis Associazione di tipo mafioso:* chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone è punito con la reclusione da dieci a quindici anni. Coloro che promuovono, dirigono, o organizzano l'associazione sono puniti per ciò solo, con la reclusione da dodici a 18 anni. Le disposizioni del presente articolo si applicano anche alla Camorra, 'Ndrangheta ed alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso[52].

[51] E. DOLCINI-G.L. GATTA, *Codice Penale e norme complementari.* Edizione aggiornata al 22 agosto 2019, GIUFFRÈ FRANCIS LEFEBVRE.
[52] E. DOLCINI-G.L. GATTA, *Codice Penale e norme complementari.* Edizione aggiornata al 22 agosto 2019, GIUFFRÈ FRANCIS LEFEBVRE.

CONSLUSIONE

Ora al fine della mia ricerca ed esposizione della tesi posso in tutta coscienza dire che ho arricchito la mia conoscenza di cosa sia il cyberspazio, a me finora poco noto.
Ho potuto approfondire, attraverso la lettura dei testi di alcuni esperti come Lawrence Lessig, J. R. Reidenberg ed Enrico Maestri, come sia nato il cyberspazio, come sia articolato e gestito a livello giuridico, parte che a me più interessava approfondire.
Non immaginavo di trovare tante forme diverse di pensiero e di persone che ne dettano leggi e/o limiti di gestione.
E 'stato importante per me, approfondire la mia conoscenza durante la lettura delle opere e delle varie teorie incontrate al riguardo di internet e del cyberspazio, perché questo ha contribuito ad arricchire, quelli che prima erano per me una conoscenza ed un pensiero di essi superficiale.
Mi ha colpito molto il confronto che Reidenberg ha posto in essere con riferimento alla regolamentazione giuridica ed alla Lex informatica. Ho sempre pensato che Internet fosse regolamentato in tutto e per tutto solo dai vari stati e non che potesse avere, sotto certi aspetti, una sua architettura ed un suo codice che gli permettessero di autoregolamentarsi.
Sono rimasta stupita di come la legge, che vige all'interno di uno stato, possa a volte, difronte al cyberspazio, diventare piccola e a tratti impotente, nell'affrontare certe dinamiche che hanno luogo all'interno di questo spazio senza confini; soprattutto di come a causa della continua e veloce evoluzione di internet e della tecnologia, le istituzioni del nostro ordinamento e non solo, siano sempre molto indietro, nel disciplinare e cercare di prevenire la realizzazione dei vecchie e nuove tipologie di illeciti che possono avere luogo nel cyberspazio.
Con riguardo a ciò, ho maturato l'idea di trattare, il tema della criminalità organizzata informatica, durante la lettura di alcune delle fonti studiate per la realizzazione di tale elaborato. Questo non solo per la curiosità e la sensibilità che tale argomento ha suscitato e continua a suscitare in me, ma anche per l'attenzione che ho sempre dato, al tema della lotta alla criminalità organizzata, sorta da parecchi anni e coltivata, grazie alla mia partecipazione da quasi un anno, alle attività dell'associazione "Libera contro le Mafie".

Giovanni Falcone diceva che, la mafia è un fatto umano e che, come tutti i fatti umani, ha un inizio e avrà anche una fine. Credo che questa sua idea possa essere non solo applicata al fenomeno mafia, ma a qualsiasi altro fenomeno caratterizzato dall'intervento dell'uomo, come ad esempio il crimine informatico.

Confido e credo che, grazie alla collaborazione che negli ultimi anni c'è stata e che ci sarà, tra gli stati membri dell'Unione Europea e tra Unione Europea e il resto del mondo, questo ritardo e questa difficoltà, nel disciplinare questi vecchi e nuovi problemi, possano essere, non dico sanati, ma ridotto il più possibile. Questo perché si possa garantire a tutti noi, che ogni giorno ormai siamo a contato con la tecnologia e internet, di poter utilizzare tutte queste risorse nel modo più sicuro e fruttuoso possibile.

BIBLIOGRAFIA

BENEDIKT, M. *Cyberspace: primi passi nella realtà virtuale.* F. Muzzio, Padova 1993.

CAVALLO M., *Internet governance: the evolution of theories of governing cyberspace.* 14 Maggio 2020

CONTI G.L., *La Lex informatica, in Osservatorio sulle fonti*, n 1/2021. Disponibile in: http://www.osservatoriosullefonti.it

DOLCINI E. - GATTA G.L., *Codice Penale e norme complementari.* Edizione aggiornata al 22 agosto 2019, GIUFFRÈ FRANCIS LEFEBVRE.

GOLDONI M., *Politiche del codice. Architettura e diritto nella teoria di Lessig*.

ILARDA G. e MARULLO G., (a cura di) *Cybercrime: Conferenza Internazionale. La convenzione del Consiglio d'Europa sulla Criminalità Informatica.* Milano, GIUFFRÈ EDITORE 2004.

MAESTRI E., *Lex informatica. Diritto, persona e potere nell'età del cyberspazio.* Edizioni scientifiche Italiane, 2015

MAESTRI E., *Lex Informatica e soft law. Le architetture normative del cyberspazio,* settembre 2017.

MAUGERI A. M. (a cura di), *Stati Generali della Lotta alle Mafie, Tavolo XV- "Mafie e Europa",* in Diritto Penale contemporaneo, 2019

MORO P., SARRA C., *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Franco Angeli 2017.

MURRAY A., *The Regulatory Edge of the Internet.* International Journal of Law and Information Technology, Vol. 11 No. 1, Oxford University Press 2003.

PICOTTI L., *Il diritto penale dell'informatica nell'epoca di Internet.* Dipartimento di scienze giuridiche Università di Trento. CEDAM 2004.

REIDENBERG J.R., *Lex Informatica: the formulation of Information Policy Rules through Technology,* 76 Tex. L. Rev 553 (1997-1998)

RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli.* Edizioni Laterza, 2014.

SITOGRAFIA

https://www.treccani.it/enciclopedia/libertarismo/

www.procura.milano.giustizia.it/reati-informatici.html

https://www.interno.gov.it/it/notizie/cybercrime-operazione-emma-contro-i-money-mules-81-arresti

R. RIJTANO, *Truffe online, cyber riciclaggio e narcotraffico: la criminalità organizzata si reinventa.* Lavialibera, 23 settembre 202, https://lavialibera.it/it-schede-690-

https://www.zerottonove.it/operazione-jamm-jamm/

https://www.diritto.it/il-principio-di-territorialità-in-diritto-penale