



Dipartimento di Giurisprudenza

Cattedra di Neuroscienze e diritto

SOCIAL ENGINEERING –

IL CONTRIBUTO DELLE NEUROSCIENZE ALLA *CYBERSECURITY*

Relatore

Chiar.ma Prof.ssa

Alessia Farano

Candidata

Gaia Buoni

Matr. 150703

Correlatore

Chiar.mo Prof.

Lorenzo D'Avack

Indice Sommario

<i>INTRODUZIONE</i>	4
<i>CAPITOLO I</i>	7
<i>SOCIAL ENGINEERING AND BEHAVIORAL ECONOMICS</i>	7
<i>1.1 Definizione e introduzione all'ingegneria sociale</i>	7
<i>1.2 Teoria del nudge</i>	11
<i>1.2.1 La mosca dell'Amsterdam airport of Schiphol</i>	18
<i>1.2.2 Architettura delle scelte ed esempio Carolyn</i>	20
<i>1.3 Pro e contro alla teoria del nudge</i>	23
<i>1.4 Nudge e diritto</i>	26
<i>1.5 Paternalismo libertario</i>	29
<i>1.6 Applicazione dell'ingegneria sociale al mondo informatico</i>	33
<i>CAPITOLO II</i>	38
<i>LE NEUROSCIENZE PER COMPRENDERE L'INGEGNERIA SOCIALE</i>	38
2.1 Neuroscienze ed emozioni.....	38
2.2 Anatomia e fisiologia delle emozioni.....	47
2.3 Ruolo delle emozioni nella teoria giuridica.....	49
2.3.1 La forza delle emozioni nel processo.....	54
2.3.1.1 "Justice is what the judge ate for breakfast".....	57
2.3.2 Neuroscienze e accertamento della responsabilità e dell'imputabilità; Sentenza Trieste..	59
2.3.3 (Segue) ... Ulteriori riferimenti giurisprudenziali sul tema dell'accertamento della responsabilità.....	65
a) Sentenza n. 536/2011 del Tribunale di Como.....	65
b) Sentenza n. 296/2013 del Tribunale di Venezia.....	67
2.4 Emozioni, informatica ed ingegneria sociale.....	71

<i>CAPITOLO III</i>	78
<i>CYBERSECURITY E RESPONSABILITÀ IN RETE</i>	78
3.1 Introduzione alla <i>cybersecurity</i> : nascita e sviluppo del <i>cyberspace</i>	78
3.1.1 Tipologie di <i>cyberattacks</i>	83
3.1.1.1 <i>Malware</i>	85
3.1.1.2 <i>Ransomware</i>	86
3.1.1.3 <i>Phishing</i>	88
3.1.1.4 <i>Pharming</i>	90
3.2 Dalla <i>cybersecurity</i> al <i>cybercrime</i> : criminalità informatica	91
3.2.1 Reati informatici nel diritto	93
3.3 <i>Cyberattacchi</i> e Covid-19: virus a confronto.....	96
3.3.1 Danni subiti dalle aziende: strategie e modelli organizzativi per le imprese	98
<i>CONCLUSIONE</i>	101
<i>BIBLIOGRAFIA</i>	105
<i>GIURISPRUDENZA</i>	113

INTRODUZIONE

L'avvento della tecnologia ha rappresentato una svolta epocale nel mondo del diritto. La crescente dipendenza da essa nella vita quotidiana ha portato ad un corrispondente aumento dei rischi a livello informatico. In particolar modo, l'ingegneria sociale, fenomeno in rapida crescita nel campo della *cybersecurity*, è diventata una delle principali preoccupazioni per gli esperti di tale ambito, poiché si basa sulla manipolazione delle vulnerabilità psicologiche ed emotive degli individui per ottenere, in questo caso, l'accesso a informazioni sensibili.

La scelta di questo argomento di approfondimento deriva dal particolare interesse che chi scrive ha manifestato durante il corso di laurea, in particolar modo perché intreccia la materia giuridica con tematiche del tutto diverse e nuove rispetto agli schemi classici del diritto.

Nel tentativo di fornire un'analisi adeguata circa le maggiori criticità della questione, l'elaborato esplora la connessione tra i principi delle neuroscienze e le tattiche utilizzate dai criminali negli attacchi di ingegneria sociale.

Lo scopo di questa ricerca è quello di comprendere più a fondo i meccanismi psicologici che spingono gli individui a cadere vittime di questi particolari attacchi.

Attraverso una panoramica non esaustiva della letteratura e dei casi di studio, questa tesi non vuole solo offrire una panoramica su quanto già esposto da illustrissimi autori, ma si pone l'obiettivo di fornire una visione dei metodi utilizzati dagli aggressori, nonché dei fattori cognitivi ed emotivi che rendono gli utenti della rete suscettibili a questi tipi di attacchi.

Partendo dal titolo, l'elaborato ha l'intento di evidenziare, sin da subito la stretta relazione che vi è tra la conoscenza informatica e le neuroscienze, il connubio quindi tra essa e la *cybersecurity*.

La presente trattazione si articola in tre capitoli.

Il primo capitolo, intitolato *Social engineering and behavioral economics*, si apre con un'introduzione all'ingegneria sociale, termine concettualizzato per la prima volta da Roscoe Pound, rinomato studioso del diritto, all'inizio del XX secolo, che descrive l'uso di tattiche psicologiche per influenzare e controllare individui e gruppi. La sua teoria fornirà le basi per comprendere i metodi utilizzati dagli aggressori negli attacchi di ingegneria sociale.

Vengono, successivamente, approfonditi il concetto di "paternalismo libertario" e la teoria del *nudge*, sviluppata dagli economisti comportamentali, al fine di capire come piccoli e sottili indizi possano influenzare il comportamento degli individui.

Il secondo capitolo, *Le neuroscienze per comprendere l'ingegneria sociale*, si concentra sul ruolo che rivestono le emozioni nella teoria giuridica.

I progressi in campo neuroscientifico permettono di comprendere il comportamento umano attraverso il funzionamento del cervello. Lo scopo di questo capitolo, quindi, è quello di chiarire, partendo dallo studio delle neuroscienze, dove e come si formano le emozioni, perché si manifestano e in che modo l'uomo può riuscire a dominarle.

Esaminando la letteratura sulle neuroscienze e analizzando alcuni casi giurisprudenziali in materia, il secondo capitolo fornisce una comprensione dei meccanismi cognitivi ed emotivi che portano gli individui a cadere vittime degli attacchi informatici. L'obiettivo finale di questa ricerca risiede nella capacità di colmare il divario tra i campi delle neuroscienze e della sicurezza informatica.

Comprendendo i fattori psicologici ed emotivi che rendono gli individui suscettibili agli attacchi di ingegneria sociale, gli esperti di *cybersicurezza* possono sviluppare strategie più efficaci per proteggere da questo tipo di minacce.

Il terzo capitolo, dal titolo *Cybersecurity e responsabilità in rete*, si propone di illustrare la materia della *cybersecurity* più specificatamente.

Partendo dal termine *cyberspace* e dallo sviluppo che esso ha subito con l'avvento di Internet, si espongono le principali minacce informatiche che in esso possono essere

perpetrate per poi soffermarsi sullo studio di alcune particolari condotte criminose che prendono il nome di *cybercrimes*.

Infine, un rapido cenno viene dedicato al significativo aumento degli attacchi informatici che si è avuto in Italia e nel resto del mondo durante la pandemia da Covid-19, a seguito della paura e della confusione, generate in un periodo nel quale, a causa del *lockdown*, la popolazione è stata costretta ancor di più a ricorrere alla rete rendendo la società più vulnerabile.

In sintesi, questa tesi fornisce una visione approfondita della connessione tra le neuroscienze, l'antropologia, la psicologia e la conoscenza informatica: ciò che rende gli attacchi informatici tanto pericolosi, infatti, è che questi non presentano alcuna specifica componente tecnica, ma sfruttano leve psicologiche come appunto, le emozioni e l'istinto.

L'obiettivo cui deve tendere lo studio di questi fenomeni è di rendere gli utenti della rete sempre più consapevoli delle suggestioni esplicite ed implicite cui siamo tutti sottoposti, per fornire efficaci strumenti di prevenzione e/o di reazione, mantenendo la mente il più possibile scevra da pressioni psicologiche e far sì che ogni condotta sia frutto di una libera scelta individuale.

Questa breve introduzione rappresenta solo un preambolo a cui seguirà la trattazione di svariati temi di impellente attualità che implicano risvolti giuridici innovativi ed interessanti.

CAPITOLO I

SOCIAL ENGINEERING AND BEHAVIORAL ECONOMICS

SOMMARIO: 1.1 Definizione e introduzione all'ingegneria sociale. – 1.2 Teoria del *nudge*. – 1.2.1 La mosca dell'*Amsterdam airport of Schipol*. – 1.2.2 Architettura delle scelte ed esempio Carolyn. – 1.3 Pro e contro alla teoria del *nudge*. – 1.4 *Nudge* e diritto. – 1.5 Paternalismo libertario. – 1.6 Applicazione dell'ingegneria sociale al mondo informatico.

1.1 Definizione e introduzione all'ingegneria sociale

L'uomo è un animale sociale e per poter sopravvivere, prosperare e ricrearsi ha bisogno della società. Una società è composta da gruppi di persone e affinché l'uomo possa sviluppare la propria personalità, essa ne diventa una condizione necessaria. Di conseguenza, la società e la vita umana viaggiano di pari passo.

Ogni persona nasce con particolari aspirazioni e aspettative che fanno parte della sua natura di base. Dall'infanzia alla vecchiaia, ogni essere umano si aspetta che i suoi bisogni vengano soddisfatti, per cui viene a crearsi un conflitto tra i suoi desideri o le sue pretese, che ricade sotto il termine di interesse.

È impossibile soddisfare tutti i desideri dell'uomo. Per questo motivo è nato il concetto di ingegneria sociale, formulato da Roscoe Pound¹ (1870-1964), per soddisfare il desiderio del massimo numero di esseri umani per il benessere della società².

Pound viene ricordato per essere stato una figura di spicco della scuola sociologica della giurisprudenza, noto soprattutto per aver sviluppato il concetto di ingegneria sociale rapportandolo con il diritto. Il suo lavoro si è concentrato sul rapporto tra diritto

¹ Giurista e teorico del diritto statunitense.

² Cfr. <https://www.lawnotes4u.in/social-engineering-by-the-roscoe-pound-sociological-school/>.

e società ed in merito egli sosteneva che lo scopo del diritto fosse quello di servire i bisogni della società e che ciò dovesse essere interpretato e applicato alla luce dei fatti sociali.

L'autore del celebre *Readings on the history and system of the common law*, dopo aver fornito la sua definizione di avvocato (colui la cui vocazione è assistere nell'amministrazione della giustizia), identifica l'ingegnere sociale:

“Per ingegnere sociale intendo, per analogia con l'ingegnere industriale, colui la cui vocazione è quella di far sì che un processo o un'attività sociale raggiunga il suo scopo con il minimo di attriti e sprechi”³.

Pound è considerato, quindi, come una delle figure più influenti della scuola sociologica di giurisprudenza per essere stato il primo a introdurre la dottrina dell'ingegneria sociale, che mira, dunque, a costruire una struttura efficiente della società che permetta di soddisfare il maggior numero di desideri con il minor numero di attriti e sprechi. Ciò comporta un riequilibrio degli interessi in competizione.

Secondo il giurista americano, la giurisprudenza sociologica dovrebbe garantire l'elaborazione, l'interpretazione e l'applicazione della legge tenendo conto dei fatti sociali.

Pound paragona il lavoro del giurista a quello dell'ingegnere: come l'ingegnere deve usare la sua abilità per fabbricare nuovi prodotti, così l'ingegnere sociale è chiamato a costruire nella società quel tipo di struttura che garantisca la massima felicità e il minimo attrito. Così facendo egli sottolinea l'importanza della formazione giuridica e del ruolo della professione legale nel plasmare la società, ritenendo che gli avvocati

³ Traduzione di: “*By social engineer I mean, on the analogy of the industrial engineer, one whose calling it is to make a social process or activity achieve its purpose with a minimum of friction and waste.*” Pound, R., *The Lawyer as a Social Engineer*, *Journal of Public Law* 3, n. 2, 1954, p. 292.

debbano essere formati come ingegneri sociali e che debbano usare la loro conoscenza del diritto per promuovere il cambiamento sociale.

La professione legale, quindi, a suo giudizio deve essere maggiormente coinvolta nell'affrontare i problemi sociali e l'educazione giuridica deve concentrarsi sull'insegnamento di come usare il diritto per migliorare la società.

Lo scopo dell'ingegneria sociale, quindi, è quello di costruire una struttura della società il più possibile scientifica.

Secondo il suo stile di pensiero, il lavoro del diritto moderno deve essere inteso come ingegneria sociale, che può quindi garantire l'equilibrio degli interessi in competizione nella società.

Egli parte dal principio per cui il diritto è l'insieme di conoscenze ed esperienze con l'aiuto delle quali viene portata avanti gran parte dell'ingegneria sociale.

La giurisprudenza diventa, così, una scienza dell'ingegneria sociale che mira a riportare equilibrio tra gli interessi in competizione nella società.

Secondo la sua teoria, l'oggetto principale del diritto è l'interesse, e l'attuazione del diritto è la soddisfazione dei desideri umani. La sua funzione è quella di effettuare una "valutazione degli interessi", in altre parole, di identificare e proteggere gli interessi che la società ritiene di maggior valore.

Nonostante risalgano alla fine del XIX secolo, le idee di Pound hanno avuto un'influenza significativa sullo sviluppo del pensiero giuridico.

Attualmente l'ingegneria sociale è strettamente legata alla sicurezza informatica di cui andremo ad occuparci più approfonditamente nei paragrafi successivi di questo elaborato.

Questo concetto, che origina dalle scienze sociali, indica qualsiasi tentativo da parte dei governi di influenzare o modellare il comportamento della popolazione. In termini più semplici, l'ingegneria sociale sfrutta la manipolazione per raggiungere determinati obiettivi che possano essere buoni o cattivi, rappresentando uno dei metodi più

semplici per raccogliere informazioni relative ad un obiettivo tramite il processo di sfruttamento della debolezza umana⁴.

L'ingegneria sociale di cui tratteremo in questo elaborato è quel ramo della sicurezza informatica che si occupa di carpire e ottenere informazioni sensibili manipolando la mente e il comportamento di chi ne ha custodia.

In un contesto di sicurezza informatica, l'ingegneria sociale viene utilizzata principalmente per indurre le vittime a rivelare dati riservati o a eseguire azioni che violano i protocolli di sicurezza, infettando inconsapevolmente i sistemi o rilasciando informazioni⁵.

È possibile, quindi, definirla come una nuova declinazione della *cyber* criminalità, connubio di sicurezza informatica e neuroscienze, vera e propria arte che sfrutta la psicologia, le vulnerabilità umane e la comunicazione interpersonale per ingannare la vittima.

Questo accade perché la nostra mente non è infallibile, anzi, spesso ci inganna e questo raggirò ha un'origine strettamente connessa all'universo delle emozioni⁶.

Come ben sappiamo la sicurezza informatica non è né un'affermazione né un punto d'arrivo; ma semplicemente un processo.

Questi “attacchi”, che tratteremo successivamente, fanno spesso leva su costrutti comportamentali e culturali per manipolare la vittima e indurla a prendere una decisione basata sulla soddisfazione (gratificazione), piuttosto che sul risultato migliore (ottimizzazione).

⁴ Conteh, N., Y., Schmick, P., J., *Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks*, International Journal of Advanced Computer Research, vol. n. 6, pp. 23-31, 2016.

⁵ Breda, F., Barbosa, H., Morais, T., *Social Engineering and cybersecurity*, 2017.

⁶ V. cap. II.

Tuttavia, l'ingegneria sociale può essere utilizzata anche per scopi "legittimi" da parte, ad esempio, dei ricercatori di mercato per raccogliere dati relativi ai sondaggi, oppure da professionisti per testare la sicurezza dei sistemi di un'organizzazione e dei loro dipendenti. L'importante è acquisire la consapevolezza dell'esistenza delle tattiche di ingegneria sociale e adottare le conseguenti misure per prevenire eventuali aggressioni, educando e formando i dipendenti sui rischi e fornendo loro una formazione su come rispondere ai tentativi di *social engineering*.

1.2 Teoria del *nudge*

Il termine ingegneria sociale può essere utilizzato anche per descrivere la *teoria del nudge*⁷ (o teoria del paternalismo libertario). L'ingegneria sociale, in questo contesto, è intesa come l'insieme dei mezzi di comunicazione messi in atto per condizionare il comportamento di una popolazione, al fine di farla agire nella direzione del suo interesse e nella direzione dell'interesse generale. È una scienza comportamentale, una teoria politica ed economica basata su suggerimenti indiretti i quali, senza forzature, influenzano il processo decisionale di gruppi ed individui a compiere determinate scelte o a modificare determinati comportamenti.

Questa teoria si basa sull'idea che le persone non sempre prendono decisioni completamente razionali e che piccoli cambiamenti nell'ambiente, noti appunto come *nudge*, possono aiutare ad orientare le scelte verso risultati più desiderabili.

⁷ Il *nudge* si basa sull'idea che le persone spesso non prendono decisioni razionali, ma piuttosto vengono influenzate da fattori come le abitudini, le aspettative e i pregiudizi inconsci. Il *nudge* mira a utilizzare questi fattori per influire sulle decisioni delle persone in modo delicato e non invasivo, senza limitare la loro libertà di scelta. Cfr. Bogliacino, F., Veltri, G., Codagnone, C., *Nudge, ovvero la "spinta gentile"*, 2016, Aggiornamenti Sociali.

Richard Thaler e Cass Sunstein⁸ nella loro opera definiscono il *nudge* ricorrendo al concetto di “architettura della scelta”⁹ che si riferisce ad una serie di elementi esterni all’individuo che possono aiutarlo o condizionarlo nelle sue scelte.

Questa architettura della scelta segue tre principi¹⁰: innanzitutto, architetture di scelte differenti generano potenziali comportamenti differenti. In secondo luogo, l’architettura della scelta è, in un certo senso, ineliminabile. Tutto viene fatto dall’uomo per giungere ad un determinato scopo. Infine, l’architettura della scelta, nonostante cerchi di delimitare i confini entro i quali dovrebbe realizzarsi il comportamento umano, non impedisce all’individuo di adottare un’opzione diversa da quella prediletta dal nudge.

Un *nudge*, dunque, è in grado di indirizzare una decisione verso un obiettivo prevedibile, nel senso che solo l’architetto della scelta, e quindi il creatore del *nudge*, potrà sapere quale sarà il risultato finale.

Il concetto del *nudging* nasce dall’unione di due termini: libertarismo e paternalismo. Il primo termine indica il diritto alla libertà di decisione dell’individuo, mentre il secondo allude ad una società che vincola gli esseri umani a regole decisionali predefinite.

⁸ Richard Thaler (1945) è un economista statunitense, considerato uno dei padri della scienza comportamentale. Cass Sunstein è un giurista e accademico statunitense, anche lui considerato uno dei padri della scienza comportamentale. Il loro libro introduce la teoria del *nudge* (spinta) al grande pubblico e fornisce esempi di come le piccole modifiche nell’ambiente possono aiutare a guidare le decisioni delle persone verso scelte più sane e sostenibili.

⁹ Thaler, R., H., Oliveri, A., Sunstein, C., R., *Nudge: la spinta gentile: la nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, Feltrinelli, 2014, pp. 91-109.

¹⁰ Pravettoni, G., *La Mente Impressionabile: Come Utilizzare Le ‘Spinte Gentili’ Per Fare Scelte Salutari*, Giornale italiano di psicologia, 2020, pp. 499-500.

Thaler e Sunstein, padri del *nudging*, creano un compromesso tra i due termini opposti, coniando l'espressione "paternalismo libertario", di cui parleremo più approfonditamente nel paragrafo successivo.

"Il paternalismo libertario consiste in quell'insieme di interventi che cercano di superare le inevitabili distorsioni cognitive e le inadeguatezze nell'assumere decisioni degli individui tenendone conto in modo da influenzare le decisioni (in un modo facilmente reversibile) e indirizzarle verso scelte che l'individuo avrebbe fatto se avesse potuto disporre senza limiti di tempo e di informazioni e se avesse avuto le abilità analitiche di un razionale decisore (più precisamente dell'Homo Oeconomicus)"¹¹.

È opportuno, a questo punto, citare due psicologi israeliani, Amos Tversky e Daniel Kahneman, facendo prima una piccola premessa.

Kahneman, sostenitore del pensiero di Thaler e Sunstein, scrisse riguardo la loro opera:

"Questo libro migliorerà le nostre decisioni. Siamo esseri umani, non calcolatori perfettamente razionali, e siamo condizionati da troppe informazioni contrastanti [...]. È per questo che abbiamo bisogno di un "pungolo", di una spinta gentile che ci indirizzi verso la scelta giusta".

A seguito di questa affermazione, però, Kahneman si chiese quanto e quale spazio rimanesse realmente per la libertà di scelta individuale.

Quindi, se da un lato i "pungoli", traduzione del termine *nudge*, si propongono come miglior mezzo per essere portati a compiere determinate scelte in un'ottica di efficienza e massimizzazione delle risorse, dall'altro il paternalismo libertario

¹¹ Cfr. Rebonato, R., *Taking Liberties: A Critical Examination of Libertarian Paternalism*, Palgrave MacMillan, London 2012, p. 6.

proposto dai due studiosi rischia di rivelarsi un mezzo di controllo e intrusione nella scelta dell'individuo circa le proprie decisioni.

Viene, a questo punto, introdotto un nuovo concetto, quello del “pensiero lento”, cioè un pensiero intenzionale, logico e riflessivo che si attiva quando viene posta l'attenzione su una scelta determinata. Si afferma, poi, la cosiddetta *teoria del doppio processo*, che ad oggi è ritenuta la spiegazione più convincente sulle modalità operative del ragionamento umano.

L'esperimento condotto dai due esperti chiarisce come il nostro cervello funzioni su due circuiti cognitivi, due sistemi responsabili delle nostre decisioni che interagiscono fra loro per rendere possibile il processo di scelta: il “sistema impulsivo” – intuitivo, automatico, veloce – e il “sistema riflessivo” – razionale, lento, riflessivo - e che le nostre scelte siano il risultato dell'attivarsi semplicemente del sistema impulsivo¹², che è rapido e viene percepito come istintivo, agisce in fretta e in modo automatico. Non necessita di grandi sforzi e non è sottoposto ad alcun tipo di controllo volontario. È grazie al sistema impulsivo che, per esempio, riusciamo a percepire istantaneamente la paura sul volto di una persona.

Il sistema riflessivo, invece, è più ponderato e consapevole. Thaler e Sunstein lo descrivono come un sistema controllato, mediato, deduttivo, lento e consapevole. È un sistema relativo ad attività mentali impegnative che richiedono una determinata concentrazione. Esso si attiva in presenza di compiti mentali più difficili e articolati, come può essere, ad esempio, la soluzione di un problema di matematica.

I neuroscienziati, studiando il cervello umano, riportano che le attività del sistema impulsivo sono associate alle parti più antiche del cervello, quelle che ci accomunano

¹² Farano, A., *L'obbedienza al diritto tra ragioni e cause*, https://iris.luiss.it/retrieve/e163de42-e367-19c7-e053-6605fe0a8397/Farano_TCRS_2021.pdf, data ultima visualizzazione 1/10/2022. Vedi anche Thaler, R., H., Sunstein, C., R., *Nudge: la spinta gentile: la nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, Feltrinelli, 2014, pp. 27-30.

ai rettili¹³. Nella psicologia questi sistemi sono chiamati, più semplicemente, “sistema 1” e “sistema 2”.

Per comprendere meglio questi concetti possiamo associare il sistema impulsivo alle reazioni viscerali e il sistema riflessivo al pensiero consapevole. I sentimenti viscerali possono essere abbastanza accurati, ma spesso inducono alla commissione di errori¹⁴ perché si tende a fare troppo affidamento sul sistema impulsivo¹⁵. I *bias* emergono, quindi, nel momento in cui il sistema 2 non riesce a percepire che vi siano degli errori del pensiero intuitivo.

I due sistemi sono perfettamente integrati tra loro al punto da non consentirci di distinguerli nel momento della loro operatività.

Il sistema 1 si fa carico del problema, nei termini in cui si presenta, e cerca subito una soluzione. Il sistema 2, invece, se necessario interviene per confermare e nel caso correggere la soluzione presa dal sistema 1.

Può capitare, però, che l'interazione tra i due sistemi dia luogo ad inconvenienti. Infatti, come abbiamo già affermato, la maggior parte dei nostri errori è il prodotto di giudizi intuitivi riconducibili al sistema 1, che non sono passati al vaglio del sistema 2. Se quest'ultimo resta, infatti, passivo, finiamo per ritenere vere impressioni che in realtà sono false. Ciò vale, soprattutto, per le scelte di vita quotidiana. Non tanto veniamo “portati fuori strada” da ciò che non sappiamo, ma da ciò che, sbagliando, crediamo di sapere¹⁶.

¹³ Lieberman, J., *Head Over the Heart or Heart Over the Head? Cognitive Experiential Self-Theory and Extralegal Heuristics in Juror Decision Making*, Journal of Applied Social Psychology, 2002.

¹⁴ Gli errori mentali a cui questi meccanismi possono portare prendono il nome di *bias*.

¹⁵ Thaler, R., H., Oliveri, A., Sunstein, C., S., *Nudge: la spinta gentile: la nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, Feltrinelli, 2014, p. 29.

¹⁶ Forza, A., Menegon, G., Rumiati, R., *Il giudice emotivo. La decisione tra ragione ed emozione*, Il Mulino, Bologna, 2011, pp. 126-127.

Questo esperimento porta a ritenere che il sistema 1 intervenga falsando la correttezza del ragionamento senza una valutazione razionale. L'idea di fondo è che le nostre decisioni siano inficiate da errori di ragionamento, difetti comportamentali che producono euristiche intuitive a discapito delle nostre capacità deliberative più razionali¹⁷.

Possiamo affermare che sia l'intuito a guidarci e alle volte ad esso non sappiamo resistere, anche quando possiamo essere perfettamente consapevoli della sua azione, ma non per questo appare possibile sottrarvisi.

Il miglior modo per comprendere questa irresistibilità è il riferimento all'illusione ottica riportata in figura.

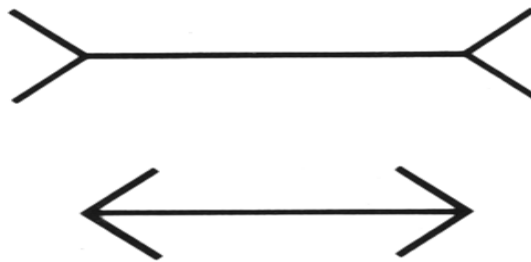


Fig. 1. Illusione di Müller-Lyer

Se, guardando l'immagine dell'illusione di Müller-Lyer, fossimo chiamati a stabilire quale tra le due linee sia la più lunga, risponderemmo immediatamente che sia la prima, anche se le linee in realtà, se misurate con un righello, risultano perfettamente uguali.

¹⁷ Galletti M., Vida S., *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, Roma, 2018, pp. 23-24.

Anche una volta ammesso che le linee sono uguali (dopo aver attivato il sistema 2 e misurato con il righello), non è possibile impedire al sistema 1 di continuare a vedere il segmento superiore più lungo di quello inferiore.

“In modo simile alle illusioni ottiche operano le illusioni del pensiero, cioè quelle procedure di pensiero che producono distorsioni come nelle euristiche di giudizio.

Queste illusioni sono spesso difficili da prevenire, poiché il sistema 1 agisce automaticamente e non può essere disattivato a piacere. Non si possono evitare gli «errori», perché il sistema 2 a volte non ha alcun indizio, e una vigilanza continua non è sempre positiva. Sicuramente, sarebbe poco pratica. Se infatti mettessimo costantemente in discussione il nostro stesso pensiero, l'esistenza sarebbe insopportabile. Il sistema 2 è troppo lento per sostituirsi al sistema 1 e fungere da incaricato principale nelle decisioni di routine. Quello che tuttavia possiamo fare è imparare a riconoscere le situazioni in cui è probabile si verifichino errori e impegnarci di più ad evitare grossi sbagli, soprattutto quando la posta in gioco è alta”¹⁸.

Concludiamo, quindi, che in base allo schema proposto da Kahneman e Tversky, la nostra capacità decisionale impulsiva (il sistema 1), prevale sulla facoltà più razionale (il sistema 2), producendo errori di giudizio potenzialmente lesivi del nostro benessere. Successivamente a questi esperimenti, Thaler e Sunstein hanno prefigurato due idealtipi: l'*homo oeconomicus*, soggetto caratterizzato da perfetta razionalità, autore di sole scelte riflessive vagliate dal sistema 2; e l'*homo sapiens*, soggetto invece, alle euristiche e alle distorsioni cognitive, esposto al potere di continui pungoli e autore di scelte irriflesse prodotte dal sistema 1. A differenza dell'*homo oeconomicus*, l'*homo*

¹⁸ Forza, A., Menegon, G., Rumiati, R., *Il giudice emotivo. La decisione tra ragione ed emozione*, Il Mulino, Bologna, 2011, p. 129.

sapiens sbaglia in modo prevedibile. L'*homo oeconomicus*, invece, per essere considerato tale deve essere in grado di fare previsioni non distorte.

Leggendo un manuale di economia, scopriamo che l'*homo oeconomicus* è un soggetto puro e ideale, dotato di perfetta razionalità e informazione totale, ma le persone che conosciamo non sono così, appartengono alla specie dell'*homo sapiens*.

Per riferirsi a questa distinzione vengono utilizzati i termini “Econi” e “Umani” tramite i quali si contrappone la concezione tradizionale del comportamento umano, perfettamente razionale e le evidenze provenienti dalla psicologia cognitiva e dall'economia comportamentale.

Il fattore emotivo gioca un ruolo fondamentale all'interno della teoria del nudge, motivo per cui le persone non sempre prendono decisioni completamente razionali. Avremo modo, nel corso del secondo capitolo di questo elaborato, di analizzare più nel dettaglio il ruolo delle emozioni e il rapporto che esse hanno con l'ingegneria sociale.

1.2.1 La mosca dell'*Amsterdam airport of Schiphol*

Un esempio simpatico e curioso per spiegare il concetto di *nudge* e come queste tecniche di ingegneria sociale abbiano portato a risultati positivi è quello della mosca negli orinatori pubblici dell'aeroporto.

Thaler considera questa storia uno degli esempi più appropriati per spiegare il concetto di *nudge*.

Da ormai diversi anni, nell'aeroporto olandese di Amsterdam possiamo trovare, applicata nei bagni degli uomini, l'immagine di una piccola mosca nera su ogni orinatoio.

Il compito di questo adesivo è quello di limitare la fuoriuscita di urina, poiché sembrerebbe che, chi usufruisca del bagno non presti molta attenzione a dove mirare e che vedendo, invece, un obiettivo, faccia maggior attenzione.

La scelta di usare una mosca deriva dal fatto che questa sia piccola e fastidiosa, ma non paurosa come può, invece, essere un ragno.

Sarebbe stato possibile apporre semplicemente delle regole all'interno dei bagni e assumere personale per farle rispettare, sanzionando i trasgressori, ma questo sarebbe risultato dispendioso. Gli adesivi, invece, hanno permesso di svolgere lo stesso lavoro senza alcun elemento di coercizione, rendendo così più facile per le persone fare la scelta giusta.

Questo esperimento, ideato da Aad Kieboom, economista e responsabile dell'espansione delle strutture dell'aeroporto, ha portato a risultati superiori rispetto ad ogni previsione, in quanto i comportamenti poco igienici sono diminuiti dell'80%¹⁹ e questo ha portato ad una riduzione delle spese di pulizia dei bagni dell'aeroporto.

Doug Kempel, imprenditore e ingegnere, ha trasformato l'esperimento della mosca in un piccolo business, vendendo online adesivi di mosche e affermando: *“Il mio obiettivo è niente meno che salvare il mondo, un orinatoio alla volta. Sono fermamente convinto che questo semplice prodotto possa rendere le toilette più pulite e più sicure. Minori pulizie vuol dire un minore uso di detergenti dannosi. E il fatto che faccia ridere non è certo un male”*²⁰.

Possiamo, quindi, affermare che queste tecniche di ingegneria sociale sfruttano con efficacia le euristiche e la relazione tra pensiero e azione, arrivando a stimolare il comportamento umano “inconsiamente”.

Le persone sottoposte a queste tecniche, infatti, non si rendono conto della situazione che si viene a creare, poiché mediante i *nudge* vengono sfruttati i c.dd. *bias cognitivi*, cioè gli errori involontari che commette la mente quando viene presa una decisione,

¹⁹ Cfr. <http://www.coathanger.com.au/archive/dibblys/loo.htm>.

²⁰ Thaler, R., H., Oliveri, A., Sunstein, C., R., *Nudge: la spinta gentile: la nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, Feltrinelli, 2014, pp. 93-94.

distorsioni che spingono a ricreare una propria visione soggettiva che non corrisponde fedelmente alla realtà.

1.2.2 Architettura delle scelte ed esempio Carolyn

Un ulteriore esempio, semplice e immediato, per capire al meglio il concetto di *nudge* e per fornire una definizione di “architetto delle scelte” è descritto nelle pagine introduttive dell’opera di Thaler e Sunstein²¹.

Carolyn, dopo aver studiato scienze della nutrizione, è diventata dirigente del servizio mensa del sistema scolastico di una grande città, e quindi responsabile di diverse scuole. Una sera, insieme ad un amico decide di condurre alcuni esperimenti nelle scuole per stabilire se la maniera di disporre e presentare gli alimenti influisca sulle scelte dei bambini. Viene, quindi, considerata un architetto delle scelte dal momento in cui, posizionando, ad esempio la frutta e la verdura all’altezza degli occhi dei bambini, li ha diretti verso una dieta più salutare, riuscendo così ad incrementare il consumo di questi alimenti addirittura del 25%.

“Da questo esperimento Carolyn ha imparato una lezione importante: i bambini, al pari degli adulti, possono essere enormemente influenzati da piccoli cambiamenti del contesto. Questa influenza può essere esercitata a scopi positivi o negativi: per esempio, Carolyn adesso sa di poter indurre i bambini a consumare più alimenti sani e meno alimenti nocivi”²².

²¹ *Ibidem.*

²² Thaler, R., H., Oliveri, A., Sunstein, C., R., *Nudge: la spinta gentile: la nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, Feltrinelli, 2014 p. 7.

Con questo esempio si arriva a delineare il concetto di “architetto delle scelte”. Un architetto delle scelte viene definito tale quando ha la responsabilità di organizzare il contesto nel quale gli individui prendono decisioni e questo porta ad affermare che Carolyn ricopra questo ruolo.

Anche nella quotidianità possiamo renderci conto che molte persone assumono la posizione di architetto delle scelte, spesso senza nemmeno rendersene conto. Un medico, ad esempio, che descrive ad un paziente i possibili trattamenti cui può sottoporsi è un architetto delle scelte; allo stesso modo lo è un genitore che descrive ai figli le diverse opzioni per l’istruzione. È un architetto delle scelte persino un addetto alle vendite in un negozio.

“[...] piccoli dettagli apparentemente insignificanti possono avere una notevole influenza sul comportamento individuale. Una buona regola pratica è ipotizzare che “ogni dettaglio conta”. In molti casi, il potere di questi particolari deriva dal focalizzare l’attenzione degli utenti in una certa direzione. [...] L’idea che “ogni dettaglio conta” può essere paralizzante, ma è anche fonte di potere. [...] E come un architetto edile, a conti fatti, deve progettare un edificio con un certo tipo di caratteristiche, così un architetto delle scelte come Carolyn deve scegliere una particolare disposizione degli alimenti disponibili per pranzo, influenzando, in questo, ciò che i bambini mangiano. Carolyn può pungolare”²³.

²³ Il termine “pungolare” viene utilizzato come traduzione di “to nudge”. Un “pungolo”, quindi, proprio come un “nudge” è qualsiasi aspetto della presentazione delle scelte che condiziona il comportamento degli individui, senza vietare però alcuna possibilità. La definizione sembra essere adatta anche per “incentivo”. Ma optare per questo termine implica una connotazione quasi esclusivamente economica, mentre un *nudge* è una spinta gentile in senso molto più ampio, che racchiude tutti i campi dell’esistenza.

La teoria del *nudging* e il fondamentale ruolo che in essa riveste l'architettura non sono conciliabili con i principi tipici della teoria economica classica²⁴ poiché – come ribadito precedentemente – una persona dotata di piena razionalità non dovrebbe essere in nessun modo suggestionabile dalla modalità di esposizione delle opzioni. Invece, secondo la *behavioral economics*, la teoria comportamentale moderna, affermatasi successivamente negli anni, le preferenze del decisore possono essere alterate o indirizzate dal numero di scelte possibili, dalla modalità con cui queste opzioni vengono esposte e dalla presenza o meno di regole di default. Questa diversa teoria, quindi, prende fortemente in considerazione l'aspetto umano del processo decisionale. Questa non solo comprende come le limitazioni alla razionalità esistano e siano scatenate da una moltitudine di situazioni, ma soprattutto coglie come gli egoismi individuali intervengano concretamente nei processi economici e decisionali e vadano, dunque, inseriti all'interno del contesto di analisi.

Già intorno agli anni '50 dello scorso secolo, veniva posta l'attenzione su questo aspetto della realtà. George Katona²⁵, nella prefazione a *Psychological Analysis of economic behavior*, proponeva un modello di analisi economica che tenesse in considerazione l'influenza del comportamento umano sull'economia e come le dinamiche logico-razionali non influenzassero gli attori economici quanto i fattori ambientali, le motivazioni e gli aspetti psicologici²⁶.

²⁴ Secondo questa teoria, l'individuo (*homo oeconomicus*) agisce per massimizzare la propria utilità in maniera del tutto asettica, non condizionato dall'ambiente esterno e dalla scarsità di risorse quali tempo e spazio. Uno dei principali assunti della teoria economica classica consiste nell'osservare una perfetta razionalità e capacità di scelta informata nei comportamenti degli agenti economici. Cfr. Daft, R. L., *Organizzazione aziendale*, Apogeo Education, 2017, cap. 12.

²⁵ George Katona (1901-1981) è stato un economista e psicologo statunitense, noto per i suoi contributi alla comprensione del comportamento economico del consumatore.

²⁶ Katona G., *Psychological Analysis of economic behavior*, McGraw-hill, 1951.

Anche autori più recenti, quali Sunstein e Thaler, espongono l'argomento, come è stato trattato nel par. 1.2 di questo elaborato. Essi, infatti, sostengono che “le persone che conosciamo” non appartengono alla specie dell'*homo oeconomicus*, ma a quella dell'*homo sapiens*²⁷.

Sottolineano, ancora una volta, l'imprecisione e l'irrazionalità delle previsioni umane, che si rivelano distorte e difettose.

Tornando al discorso precedente, un'architettura delle scelte, per essere efficace, deve influenzare indirettamente le decisioni altrui. Molte persone, generalmente, scelgono le opzioni che richiedono il minimo sforzo, in quanto l'inerzia (principio psicologico alla base del comportamento umano che analizzeremo nel capitolo seguente) svolge un ruolo fondamentale nella presa delle decisioni.

Al fine di dare una precisa definizione al concetto, si ritiene che un buon sistema di architettura delle scelte sia tale quando aiuta gli individui a perfezionare la propria capacità di mappare le decisioni e, dunque, scegliere le opzioni che possano accrescere il loro benessere.

1.3 Pro e contro alla teoria del *nudge*

Dopo aver analizzato la teoria del *nudge*, occorre esaminare le tesi a favore e quelle contrarie a questo fenomeno. A riguardo, distinguiamo i sostenitori dei *nudge* dai cosiddetti “oppositori di pungoli”.

Come già affermato precedentemente²⁸, uno dei primi sostenitori del *nudge* e del pensiero di Thaler e Sunstein è Kahneman, secondo cui l'opera dei citati autori (e

²⁷ Thaler, R., H., Oliveri, A., Sunstein, C., R., *Nudge: la spinta gentile: la nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, Feltrinelli, 2014.

²⁸ Cfr. par. 1.2.

quindi la relativa teoria) migliorerebbe le nostre decisioni, grazie a “spinte gentili”²⁹ che ci indirizzano verso giuste scelte.

Un altro sostenitore della teoria di *nudge* è Barack Obama che, durante il suo mandato, aveva incaricato Sunstein di progettare alcuni *nudge* comportamentali per indirizzare i cittadini americani a “fare la cosa giusta” senza esserne costretti.

A seguito di questa iniziativa del Presidente degli U.S.A., anche la Gran Bretagna nel 2010 si è adoperata a favore del *nudging* con l’istituzione della prima *Nudge Unit* che si è occupata con successo di promuovere la donazione di organi.

Il quesito che è stato posto ai cittadini è stato se questi avrebbero voluto ricevere un organo in caso di bisogno. Risposte positive a questo interrogatorio banale hanno portato ad un incremento di iscrizioni ai registri per le donazioni di 100.000 l’anno³⁰. Agli occhi, invece, dei detrattori della teoria (i cosiddetti “oppositori di pungoli”), un primo problema di applicazione può essere quello di arrivare a trovarsi di fronte ad un’ondata di forme di *nudge* (e di paternalismo) così invadenti da diventare inaccettabili³¹, anche se Thaler e Sunstein replicano a queste critiche affermando che alla base del *nudging* vi sia proprio la condizione libertaria dell’individuo. In questo caso, si passerebbe da una propaganda governativa incentrata sull’educazione, ad una coercizione, fino ad imporre divieti, multe e persino pene detentive. Un esempio è quello relativo alle sigarette: in alcuni paesi siamo passati dai semplici messaggi di avvertimento a campagne di informazione molto aggressive fino al divieto di fumo nei

²⁹ Cfr. Par 1.4.

³⁰ Rutter, T., *The Rise of Nudge – the Unit Helping Politicians to Fathom Human Behaviour*, The Guardian, 2015, in <https://www.theguardian.com/public-leaders-network/2015/jul/23/rise-nudge-unit-politicians-human-behaviour>.

³¹ Thaler, R., H., Oliveri, A., Sunstein, C., R., *Nudge: la spinta gentile: la nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, Feltrinelli, 2014, p. 229.

locali pubblici. Ciò porta a riflettere circa la possibilità che questi paesi possano, prima o poi, adottare regole ancora più severe e bandire del tutto il fumo.

Un secondo problema di applicazione diverso dal precedente viene sollevato da altri critici³² del pensiero di Thaler e Sunstein. Questi disapprovano ogni provvedimento pensato esplicitamente per aiutare persone poco istruite. Costoro criticano questi provvedimenti perché convinti che qualsiasi forma di assistenza nei confronti di questi soggetti debba provenire volontariamente dal settore privato. Più semplicemente la critica è rivolta all'intervento pubblico che sottrae risorse a qualcuno in favore di altri. Riguardo questa condanna, Thaler e Sunstein spiegano che in verità questi pungoli aiutano chi ha bisogno determinando un costo trascurabile per chi invece non ne abbia (ad esempio una campagna per aiutare a smettere di fumare non causerà problemi a chi già non fumi).

Alcuni diffidenti potrebbero ritenere che, in una società libera, le persone abbiano il pieno diritto di avere torto e che, anzi, sia utile commettere errori perché “sbagliando si impara”.

Anche L. Savadori³³ nell'articolo “*Nudge: opportunità o moda passeggera?*”³⁴, sostiene che, al giorno d'oggi, le tecniche di *nudging* stiano riscontrando un notevole

³² Cfr. Gigerenzer Gerard, il quale sostiene che i *nudge* possono essere inefficaci o addirittura dannosi se le persone non capiscono o non accettano le scelte che vengono loro presentate; Glennerster Rachel, economista dello sviluppo presso l'Università di Cambridge, ha messo in dubbio l'efficacia dei *nudge* come strumento per affrontare problemi sociali complessi come la povertà e l'insicurezza alimentare; lo stesso Sunstein ha espresso alcune preoccupazioni riguardo alla possibilità che i *nudge* possano essere troppo paternalistici e limitare la libertà individuale.

³³ Professore Associato del dipartimento di Economia e Management dell'Università di Trento.

³⁴ Savadori, L., *Nudge: opportunità o moda passeggera?*, Giornale italiano di psicologia, Rivista trimestrale, 2/2020, pp. 355-376, <https://www.rivisteweb.it/doi/10.1421/97859>, data ultima visualizzazione 14/11/2022.

successo in tutto il mondo. Tuttavia, un così rapido aumento di notorietà deve far riflettere di fronte al fatto che i meccanismi psicologici che fanno funzionare un *nudge* non siano sempre noti.

Inoltre, la preoccupazione espressa da L. Savadori è che la teoria di *nudge* sia solo una moda passeggera e che ci sia sempre il rischio che questa venga travolta da un calo di credibilità.

1.4 Nudge e diritto

Un aspetto che, generalmente, viene trascurato riguarda il tema della giuridicità del *nudge*. È necessario, quindi, chiarire se e a quali condizioni esso sia categorizzabile come strumento giuridico.

Il problema che viene, qui, affrontato non è solo quello relativo all'efficacia giuridica del *nudge*, ma anche la questione della sua legittimità e della legittimazione di politiche pubbliche concepite a partire dagli esiti delle scienze comportamentali³⁵.

Per addentrarsi nell'analisi della natura giuridica del *nudge* è necessario riprendere la riflessione sul carattere perfezionistico del paternalismo libertario (che verrà trattato nel paragrafo successivo, 1.5), mostrando le incertezze che esso genera³⁶.

³⁵ In questo, è incoraggiante la natura dei più recenti contributi di Sunstein, tra cui: Sunstein, C., R., *Nudges vs. shoves*, Harvard Law Review, 127, 6, 2014, pp. 210-217; Id., *Do People Like Nudges?*, Administrative Law Review, 68, 2, 2016, pp. 177-232; Id., *Regulation as delegation*, Journal of Legal Analysis, 7, 1, 2015, pp. 1-36; Id., *Nudges that Fail*, Behavioural Public Policy, 1, 1, 2017, pp. 4-25; Sunstein, C., R., *Is Cost-Benefit Analysis a Foreign Language?*, Quarterly Journal of Experimental Psychology, 2017, <http://nrs.harvard.edu/urn-3:HUL.InstRepos:34337424>.

³⁶ Galletti M., Vida S., *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, Roma, 2018, pp. 301-303.

La complessa relazione che lo strumento del *nudge* intrattiene con il concetto di benessere, proposto dal paternalismo libertario, ha importanti connessioni sull'ambigua natura normativa di esso.

Inoltre, il confronto tra la teoria del *nudge* e la concezione della normatività da un lato, e la riflessione sull'effettività della regolazione dall'altro, hanno reso più difficile rispondere alla domanda se il *nudge* abbia o meno natura giuridica³⁷.

La letteratura sul *nudging* accoglie, implicitamente, l'idea che il *nudge* sia affine al diritto. Tuttavia, se si parte dalla considerazione che il diritto sia tipicamente legislativo e coercitivo, mentre il *nudge* un dispositivo “*soft*”, la possibilità di ricondurlo nella sfera giuridica sembra minacciata. Nonostante ciò, il rapporto tra legge e *nudge* è controverso per ragioni che hanno a che fare con altri requisiti della giuridicità rispetto ai quali le spinte gentili, anche se dispositivi “*soft*” di influenza della condotta, sembrano essere forme di condizionamento addirittura più efferate della legge³⁸.

Nell'ultimo decennio i teorici del *nudge* (Sunstein e Thaler) si sono impegnati nella predisposizione di una “*nudge agenda*”³⁹. Tuttavia, nei loro scritti non si concentrano sulla natura normativa e/o giuridica del *nudge*; vi sono numerosi argomenti trattati, ma non viene rinvenuto nessun approfondimento riguardo la teoria delle norme, solo pochi riferimenti alle questioni costituzionali.

³⁷L'attribuzione di una natura “extra-giuridica” al *nudge*, visto come “*techno-regulation and mandatory disclosure*”, è esplicita in Calo, *Code Nudge, or Notice?*, cit., anche se la sua riflessione può essere intesa come un tentativo di riflettere sulla possibilità che il *nudge*, ma anche altri meccanismi “*non-legal regulatory*”, possano essere considerati entro od oltre il paradigma del diritto come legge.

³⁸ Cserne, P., *Is Nudging Extra-legal?*, p. 160.

³⁹ Secondo la terminologia usata da Angner, E., in *Behavioral Welfare Economics, Libertarian Paternalism, and the Nudge Agenda*, GMU Working Paper in Economics, n. 15-29, 2015, <https://ssrn.com/abstract=2580523>, data ultima visualizzazione 21/11/2022.

Questa singolare lacuna si comprende nel momento in cui si riflette che la questione, per la cultura liberale americana, non è tanto spiegare cos'è il *nudge*, quanto piuttosto rassicurare sul suo carattere tendenzialmente paternalistico. Quindi, pur essendo vero che Sunstein ha sempre risposto alle critiche di coloro che in questo strumento e nel paternalismo vedono un pericolo per la democrazia, sono tuttavia rimaste inevase alcune domande, tra cui quella relativa alla controversa giuridicità delle spinte gentili. Prima di approfondire “fenomenologicamente” il tema della presenza del *nudging* nel nostro ordinamento, è quindi fondamentale l'esigenza di chiarire la natura giuridica del *nudge*. Da un lato, esso viene considerato troppo “*soft*”, come menzionato all'inizio del paragrafo, per essere considerato diritto in senso proprio; dall'altro, con la premessa che il diritto in quanto legge sia coercitivamente strutturato, porterebbe a ritenere che una spinta gentile (non coercitiva) non possa essere definita come un dispositivo giuridico a tutti gli effetti. La normatività del *nudge*, quindi, continua ad eccedere dai *framework* tipici della teoria del diritto.

Secondo una diversa tradizione, la sua giuridicità è legata ad assunzioni sul tipo di soggetto o agente umano per il quale è concepita. Le norme, infatti, sono predisposte per soggetti le cui razionalità sono limitate, ma mai messe in dubbio. Pertanto, le scienze comportamentali perfezionano le tecniche di manipolazione dell'architettura della scelta che contraddicono le ipotesi relative alla capacità di decidere, di far accadere gli eventi. Alcune di queste tecniche sembrano funzionare grazie alla manipolazione delle condotte di modo che gli individui siano indotti a scegliere in un determinato modo. In questi casi, che vi sia un *nudge* o altro, siamo di fronte ad un caso di ingegneria sociale che contrasta con il presupposto liberale che il diritto sia una guida normativa della condotta. In questo caso la domanda relativa alla giuridicità

del *nudge*, anche quando questo non sia in grado di rappresentare una guida normativa della condotta, è inevitabile⁴⁰.

L'analisi del rapporto tra *nudging* e diritto dimostra che i processi di legittimazione cui è sottoposto il diritto non sono un problema effettivo per il *nudge*. Lo rivela indirettamente Sunstein⁴¹, secondo il quale il *nudging* non sempre ha bisogno del diritto. Normativamente parlando, il *nudge* è indipendente e non implica interferenze autoritarie nelle condotte delle persone. Per questo motivo, può essere integrato nei nostri sistemi giuridici con o senza supporto legislativo. Nell'esempio di cui al par. 1.2.2, in particolare, non è stato chiamato in causa nessuno strumento giuridico.

Secondo gli esperti di "diritto e *nudge*", quindi, questi due concetti si incontrano in due modi: quando soggetti privati sollecitano i loro clienti a compiere comportamenti desiderabili; oppure quando enti pubblici cercano di pungolare i cittadini a tenere determinate condotte⁴².

1.5 Paternalismo libertario

Il paternalismo libertario, accennato nel paragrafo precedente, consiste nella fusione di due termini contrastanti: libertarismo e paternalismo. L'uno indica il diritto alla libertà di decisione dell'individuo, l'altro, invece, allude ad una società che vincola i soggetti a regole predefinite. Questo concetto nasce, quindi, dall'accoppiamento di due termini che sembrano evidenziare una naturale contrapposizione di idee: il paternalismo, il quale prevede l'imposizione di determinate regole che

⁴⁰ Galletti M., Vida S., *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, Roma, 2018, pp. 334-342.

⁴¹ Prefazione al libro di Alemanno e Sibony "*Nudge and the Law*".

⁴² Galletti M., Vida S., *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, Roma, 2018, pp. 360-361.

necessariamente limitano la libertà di scelta delle persone, e il libertarismo il quale, viceversa, permette alle persone di agire come meglio credono.

La natura ossimorica, nata dalla contrapposizione di idee differenti, viene spesso ripresa da Cass Sunstein e Richard Thaler.

Con il paternalismo libertario il soggetto ha a disposizione le stesse alternative, non viene imposto alcun divieto, solo piccoli pungoli che stimolano a prendere una decisione rispetto ad un'altra, una leggera spinta verso un comportamento più corretto che va a beneficio dell'individuo e della società.

L'aggettivo "libertario", quindi, vuole significare il perseguimento della libertà di scelta individuale in un contesto in cui la c.d. "architettura delle scelte"⁴³ indirizza gli individui a determinate azioni.

Il paternalismo libertario si propone di far leva su euristiche⁴⁴ e distorsioni per modificare l'architettura delle scelte.

La tesi di Thaler e Sunstein è che ogni architettura della scelta deve consentire la decisione consapevole del soggetto di accettare o meno il *nudge* proposto. A tal proposito Sunstein individua due tipi principali di paternalismo: uno debole e uno forte.

Il primo tipo, quello c.dd. "debole/*soft*", si propone di indirizzare le scelte degli individui nel compimento di atti senza limitarne la libertà di scelta. Viene, infatti, definito "libertario" perché preserva la libertà di scelta dell'individuo. I paternalisti libertari si assumono, quindi, la "responsabilità di organizzare il contesto nel quale gli

⁴³ Termine coniato da Thaler e Sunstein con cui ci si riferisce alla pratica di influenzare le scelte del soggetto decisore attraverso la modalità di esposizione delle varie opzioni.

⁴⁴ Le euristiche indicano una scorciatoia mentale che rende un processo cognitivo meno dispendioso, al fine di determinare la valutazione di un fenomeno.

individui prendono decisioni”⁴⁵, e si differenziano dai paternalisti tradizionali (c.dd. “forti/*hard*”) i quali, invece, impongono comportamenti introducendo sanzioni per far sì che vengano compiute determinate scelte.

Il paternalismo libertario, del quale si discorrerà in questa sede, si propone in maniera tale da massimizzare la probabilità che l’agente scelga quell’opzione, senza però impedirgli di agire diversamente; è un approccio che preserva la libertà di scelta individuale indirizzando le persone nella direzione che promuove il loro benessere, incoraggiandole a eseguire quello che sceglierebbero di fare se fossero nelle condizioni di optare per il meglio.

Questa serie di accorgimenti prende il nome di “spinte gentili” perché orienta gli individui a fare delle scelte senza tuttavia costringerli nel compimento; esse vengono utilizzate semplicemente per guidare le alternative delle persone.

Volendo fornire una definizione di “spinta gentile” è possibile riferirsi a Thaler e Sunstein i quali, nel corso del tempo, hanno presentato varie versioni con piccole sfumature differenti. Nel primo libro sull’argomento, la cui edizione originale è del 2008, definiscono una spinta gentile come:

“qualsiasi aspetto dell’architettura delle scelte che altera il comportamento degli individui in maniera prevedibile, senza proibire alcuna opzione o modificare in misura significativa gli incentivi economici”⁴⁶.

In base a questa definizione una spinta gentile è in grado di alterare il comportamento delle persone secondo le previsioni del cd. architetto delle scelte e non impone alcun

⁴⁵ Thaler, R., H., Oliveri, A., Sunstein, C., R., *Nudge: la spinta gentile: la nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, Feltrinelli, 2014, pp. 10-13.

⁴⁶ *Ibidem*.

costo all'agente. I costi consistono nello scegliere opzioni diverse rispetto a quella suggerita dalla spinta.

Nel 2015 Sunstein presenta una definizione di spinta gentile più o meno simile a quella riscontrata nel testo precedente, ma con l'aggiunta di una specificazione circa la meta verso cui spingere gli individui. Qui le spinte gentili sono:

“intese come iniziative che mantengono la libertà di scelte nel momento stesso in cui guidano le decisioni delle persone nella giusta direzione (secondo l'apprezzamento di queste stesse persone)”⁴⁷.

L'ultima definizione di spinta gentile, che fa riferimento a interventi che conservano la libertà di scelta, la troviamo in un libro di Sunstein del 2016. Qui le spinte gentili sono considerate come distinte, seppur complementari, rispetto agli “usi dell'architettura della scelta, intesi come condizioni di sfondo delle scelte delle persone”⁴⁸.

Queste definizioni sono accomunate dalla clausola di libertà, cioè implicano che l'uso di spinte gentili lascia agli individui la libertà di sottrarsi alla loro azione e scegliere diversamente⁴⁹.

L'obiettivo ultimo di una spinta gentile, quindi, è quello di “invitare gentilmente” l'essere umano a fare una scelta o a compiere un'azione piuttosto che un'altra, attraverso una corretta progettazione delle architetture delle scelte poiché, come

⁴⁷ Sunstein, *Effetto Nudge*, cit., p. 13. Nel testo precedente la specificazione è riferita ai provvedimenti paternalistici e non direttamente alle spinte gentili.

⁴⁸ Sunstein, C., *The ethics of influence: government in the age of behavioral science*, Cambridge University Press, 2016, p. 5.

⁴⁹ Galletti M., Vida S., *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, Roma, 2018, pp. 114-115.

vedremo nel capitolo successivo di questo elaborato, spesso le emozioni prendono il sopravvento sugli inviti rivolti all'uomo portandolo a prendere decisioni irrazionali piuttosto che a seguire i consigli dettati dalla società. Le spinte gentili permettono, quindi, di evitare questi errori indirizzando il soggetto a prendere decisioni che dovrebbero risultare migliori per sé e di conseguenza per la società.

1.6 Applicazione dell'ingegneria sociale al mondo informatico

Dopo aver elaborato un quadro principale, occorre argomentare circa la relazione che esiste tra questo meccanismo di ragionamento umano e il mondo dell'informatica, nuovo spazio sociale (terreno fertile di sviluppo) in cui si esprime l'ingegneria sociale. Internet è diventato, ad oggi, il più grande mezzo di comunicazione e di scambio di informazioni e la criminalità legata ad esso e al mondo cibernetico è classificata come "criminalità informatica". Questa rappresenta una minaccia per le economie e per la sicurezza individuale ed è stata identificata come il principale strumento di terrorismo⁵⁰.

Gli attacchi di ingegneria sociale sono in rapido aumento nelle reti odierne e stanno indebolendo la catena della sicurezza informatica mirando a manipolare individui e imprese affinché siano indotti a divulgare dati sensibili nell'interesse dei criminali informatici.

L'ingegneria sociale sta sfidando la sicurezza di tutte le reti, indipendentemente dai sistemi di rilevamento delle intrusioni e dai metodi di crittografia.

Come vedremo nel capitolo successivo, gli esseri umani sono più propensi a fidarsi di altri loro consimili rispetto ai computer o alle tecnologie e rappresentano, pertanto, l'anello più debole della catena della sicurezza. Le attività dannose compiute

⁵⁰ Lee, W., *Emerging Cyber Threats, Trends & Technologies Report*, Georgia Institute of Technology, 2018, p. 28.

attraverso le interazioni umane influenzano psicologicamente una persona a divulgare informazioni riservate o a violare le procedure di sicurezza. Grazie a queste interazioni umane, gli attacchi di ingegneria sociale minacciano sistemi e reti senza possibilità di prevenirli, utilizzando soluzioni *software* o *hardware*, finché le persone non vengono istruite a prevederli.

Nel *cyberspazio*, l'ingegneria sociale induce gli utenti a compromettere i sistemi informatici. In questo modo gli ingegneri sociali, invece degli attacchi tecnici ai sistemi, prendono di mira le persone che hanno accesso a determinate informazioni, manipolandole per indurle a divulgare notizie riservate o a portare a termine attacchi malevoli attraverso l'influenza e la persuasione.

L'ingegneria sociale viene utilizzata come metodo di attacco dominante, mediante un atto di inganno in cui gli utenti/vittime vengono manipolate al fine di rivelare informazioni ad un criminale che poi esegue determinati compiti fingendo di essere l'utente target. In questo caso il computer della vittima viene utilizzato a sua insaputa per attacchi che possono essere considerati un abuso dell'uso autorizzato.

Gli attacchi di ingegneria sociale, con il continuo evolversi del mondo informatico, stanno diventando sempre più comuni e progressivamente più sofisticati e complessi. La base consiste nell'eludere i sistemi di sicurezza informatica con l'inganno, sfruttando l'anello più debole, cioè le persone coinvolte mediante il comportamento dell'ingegnere sociale, che attraverso un'opera di persuasione, sfrutta istinti innocenti, non criminali (metodi come le minacce o la corruzione non rientrano nell'ambito dell'ingegneria sociale)⁵¹.

Secondo il Dipartimento di Giustizia degli Stati Uniti, gli attacchi di *social engineering* sono una delle minacce più pericolose al mondo. Nel 2016, la società di analisi della sicurezza informatica *Cyence* ha dichiarato che gli Stati Uniti è stato il Paese preso di

⁵¹ Breda, F., Barbosa, H., Morais, T., *Social Engineering and Cybersecurity*, 2017.

mira dal maggior numero di attacchi di ingegneria sociale e ha avuto il costo più elevato, stimato in 121,22 miliardi di dollari, seguito da Germania e Giappone⁵².

Nel capitolo successivo verrà illustrato come gli attacchi di ingegneria informatica siano in grado di influire sulla sfera emotiva delle persone, o meglio delle proprie vittime, per indurle a compiere azioni immediate, come conseguenze di emozioni non controllabili. È in questo momento che si giunge al connubio di discipline all'apparenza non connesse, quali l'informatica, la psicologia, le neuroscienze e l'antropologia. Non a caso, ciò che rende questi attacchi così dannosi è il fatto che non presentino specifiche componenti tecniche, ma che invece, sfruttino leve psicologiche come, appunto, le emozioni e l'istinto, elemento centrale del cervello rettiliano descritto da MacLean⁵³.

Questa rappresentazione si lega con quanto affermava Aristotele riguardo a *Pathos*, *Ethos* e *Logos*, tre categorie di analisi della comunicazione persuasiva⁵⁴.

Il *Pathos* allude alla capacità dell'oratore, in questo caso il criminale informatico, di suscitare emozioni e sentimenti nel pubblico.

L'*Ethos*, il secondo metodo di persuasione, è dato dal comportamento pratico in quanto oggetto dell'etica, essenziale per stimolare l'interesse di chi ascolta o di chi legge. È per questo motivo che gli attacchi di ingegneria sociale riguardano sempre argomenti sensibili, come può essere un accesso sospetto ad un conto bancario.

Infine, il *Logos*, fa riferimento al ragionamento che viene invece, impedito nelle prime due categorie di analisi della persuasione. Tuttavia, la quotidianità è influenzata molto più dalle prime due che dal *Logos*. Infatti, Aristotele nella sua retorica iniziava sempre

⁵² Salahdine, F., Kaabouch, N., *Social Engineering Attacks: A Survey. Future Internet*, 11, 89, 2019, <https://doi.org/10.3390/fi11040089>.

⁵³ Vedi Cap. 2, par. 2.4.

⁵⁴ Fagioli, S., *Filosofia retorica e logica argomentativa in Aristotele*, Torino, Giappichelli, 2022.

parlando di *Ethos*, cioè della credibilità ottenuta con il giusto stile, fondamentale per catturare l'attenzione del pubblico.

Tornando al discorso relativo all'ingegneria informatica, chi riesce a padroneggiare queste tecniche si mostra come fonte autorevole agli occhi della propria vittima, riuscendo così, a generare quel senso di urgenza che la spinge a compiere subito l'azione dannosa.

Per questo motivo, essere consapevoli di queste tecniche può essere utile ad individuare e reprimere quelli che possono essere i messaggi ingannatori, che verranno trattati più nel dettaglio nel capitolo 3 di questo elaborato.

CAPITOLO II

LE NEUROSCIENZE PER COMPRENDERE L'INGEGNERIA SOCIALE

SOMMARIO: 2.1 Neuroscienze ed emozioni. – 2.2 Anatomia e fisiologia delle emozioni. – 2.3 Ruolo delle emozioni nella teoria giuridica. – 2.3.1 La forza delle emozioni nel processo. – 2.3.1.1 *“Justice is what the judge ate for breakfast”*. – 2.3.2 Neuroscienze e accertamento della responsabilità e dell'imputabilità; Sentenza Trieste. – 2.3.3 (Segue) ... Ulteriori riferimenti giurisprudenziali sul tema dell'accertamento della responsabilità. – a) Sentenza n. 536/2011 del Tribunale di Como. – b) Sentenza n. 296/2013 del Tribunale di Venezia. – 2.4 Emozioni, informatica ed ingegneria sociale.

2.1 Neuroscienze ed emozioni

Dopo aver fornito, nel capitolo precedente, un quadro generale sull'ingegneria sociale, occorre dedicare parte dell'elaborato ai progressi in campo neuroscientifico che ci permettono di comprendere il comportamento umano attraverso il funzionamento del cervello.

L'uomo è uno degli organismi più complessi che esistano, complicato da analizzare e comprendere.

Gli studi che vengono effettuati sul funzionamento neurologico investono settori che, nonostante siano diversi per quanto riguarda l'ambito oggettivo, sono spesso accomunati da visioni unitarie su specifici argomenti.

Il fine ultimo cui cerca di arrivare questo capitolo è quello di chiarire, partendo da un approfondimento sulle neuroscienze⁵⁵, dove e come si formano le emozioni, perché si manifestano e in che modo l'uomo può cercare di dominarle.

Già nel V secolo a.C., il filosofo Alcmeone di Crotona, dopo aver sezionato degli animali, affermò che il cervello era la sede delle sensazioni, delle emozioni e del pensiero perché aveva notato in esso l'esistenza di canali in grado di trasmettergli le esperienze sensoriali e quindi capì che esisteva una correlazione tra cervello e organi di senso. Questa scoperta lo portò ad ipotizzare che anche nell'essere umano si ripettesse la medesima struttura.

Per comprendere il funzionamento neurologico e ciò che spinge l'uomo ad agire viene spesso utilizzato il parallelismo con l'animale, del resto l'uomo è un animale che si differenzia dal resto della specie per la capacità di attivare quella parte del cervello che gli permette di "ragionare" e di essere consapevole (nella maggior parte dei casi) delle azioni che pone in essere.

⁵⁵ Il neologismo "neuroscienze" compare per la prima volta nel 1972 nella formula inglese "*The Neuroscience Research Program*" (NRP) per indicare un programma di ricerca diretto da Francis Otto Schmitt al Massachusetts Institute of Technology, che riunisce biologi e scienziati di diversa formazione (come riporta Filindeu M.T., *Colpevolezza e neuroscienze: prospettive di un confronto dialogico*, in *Itinerari di Diritto Penale*, Giappichelli, Torino, pp. 2-3). Questo studioso americano si era reso conto di come lo studio del sistema nervoso abbisognasse di competenze interdisciplinari. Il *Neuroscience Research Program* (NRP) è un'organizzazione interuniversitaria e internazionale fondata nel 1962 che ha segnato un momento chiave nella fondazione delle neuroscienze quale disciplina. Attività principale del NRP è stata quella di creare collegamenti tra le scienze neurali e comportamentali (si legga anche Lattanzi N., *Verso la convergenza tra neuroscienze e intelligenza artificiale*, in *Nuova Antologia. Rivista di lettere, scienze ed arti*, Gennaio-Marzo 2020, Vol. 624, Fasc. 2293, Edizioni Polistampa, Firenze, 2020, pp. 59-75).

Lo studio del cervello, ad oggi, risulta elemento imprescindibile da cui partire, soprattutto per il campo d'indagine delle neuroscienze⁵⁶, a differenza di come accadeva nell'antichità in cui il cervello era considerato avere un ruolo secondario rispetto al cuore. Si abbandona una visione eccessivamente “romantica” dell'uomo e l'importanza che viene data al cuore nei comportamenti umani, aderendo ad una visione più “scientifica” in cui il cervello diventa elemento da studiare per comprendere i comportamenti dettati dalle emozioni.

Oggi, con il termine neuroscienze si vuole designare “*un gruppo di discipline scientifiche tra loro eterogenee*”⁵⁷, *ma che condividono un fondamentale programma comune: quello di comprendere come il cervello renda possibili i fenomeni mentali e i comportamenti umani, anche quelli più complessi e tradizionalmente considerati inaccessibili all'indagine scientifica*”⁵⁸: i processi neuronali non solo presidiano le funzioni integrative superiori, ma rappresentano il substrato organico di pensieri, emozioni e decisioni.

⁵⁶ Le neuroscienze qui sono intese come una disciplina ibrida che comprende neurologia, psicologia, neuropsicologia e neuropsicobiologia. Le neuroscienze promettono di identificare i correlati neurali di ogni attività mentale (neuroscienze cognitive) e comportamentale (neuroscienze comportamentali), nella convinzione che ad ogni funzione e contenuto mentale corrisponda l'attivazione di un'area cerebrale specifica. Cfr. Farano, A., *Emozioni e teoria del giudizio: una prima ricostruzione*, BioLaw Journal, Rivista Di BioDiritto, 2020, p. 433, <https://doi.org/10.15168/2284-4503-535>, data ultima visualizzazione 31/10/2022.

⁵⁷ Dalla *neuroscienza molecolare* alla *neuroscienza cellulare*, dalla *neuroscienza dei sistemi* alle *neuroscienze cognitive*, dalla *neuropsicologia* alle *neuroscienze comportamentali* (che hanno appunto ad oggetto i meccanismi cerebrali propri del comportamento). Anche all'interno delle cd *neuroscienze giuridiche* potrebbero distinguersi a loro volta *neuroscienze forensi*, *neuroscienze criminali*, *neuroscienze normative* e della *cognizione morale*.

⁵⁸ Bianchi, A., *Neuroscienze e diritto: spiegare di più per comprendere meglio*, in AA.VV., *Manuale di neuroscienze forensi*, Milano, 2009, XII.

Un importante lavoro di indagine delle basi neuronali e comportamentali è da attribuire ad Antonio Rosa Damasio (1944), neurologo e neuroscienziato portoghese, il quale sostiene che lo studio del cervello debba essere direttamente connesso allo studio dell'organismo al quale appartiene.

Secondo Damasio la filosofia ha influenzato per molto tempo lo studio della mente umana, facendo erroneamente credere che essa sia un'entità separata dal corpo. Invece, a suo giudizio corpo e mente costituiscono un'unità integrata rispetto a cui ogni dualismo risulta essere un'astrazione che impedisce la comprensione dei processi neurologici e mentali⁵⁹.

Di conseguenza anche le emozioni non possono essere ridotte all'attività mentale del cervello, ma sono la conseguenza di una combinazione di atti valutativi mentali.

L'ipotesi di Damasio è quella che esistano una "mente incorporata" e una continuità tra processi fisiologici, emozionali e cognitivi, con l'obiettivo di fornire una spiegazione unitaria dell'organismo attraverso una "mentalizzazione" del corpo e una "somatizzazione" della mente⁶⁰.

Ne "*L'errore di Cartesio*"⁶¹, una delle sue opere più importanti, Damasio si propone di unificare tra loro i concetti di corpo, mente e cervello, basandosi su dati principalmente scientifici.

Il neurologo portoghese cerca di dimostrare, partendo da casi clinici, che l'idea dell'esistenza di un pensiero puro, di una razionalità non influenzata da emozioni, non abbia riscontro nella realtà⁶². Gli esperimenti clinici rivelano che è quando la mente

⁵⁹ Per una panoramica sull'idea di organismo come unità integrata all'interno del pragmatismo americano cfr. Johnson, M., *Mind Incarnate: From Dewey to Damasio*, in: «Daedalus», vol. CXXXV, n. 3, 2006, pp. 46-54.

⁶⁰ Cfr. Damasio, A., *Descartes' Error*, cit.

⁶¹ Damasio, A., *Descartes' Error: Emotion, Reason, and the Human Brain*, New York, Putnam, 1994, traduzione di Mancaluso, F., *L'errore di Cartesio*, Milano, Adelphi, 1995.

⁶² Re, A., *L'errore Di Cartesio*, Ecozon@, 1.1, 2010, p. 83.

razionale mette in atto processi decisionali, in quel momento entrano in gioco i sentimenti, indispensabili per orientare l'individuo nella giusta direzione.

La scoperta dell'incidenza delle emozioni nel processo decisionale umano costituisce uno dei momenti più significativi della storia recente delle neuroscienze.

Il rendiconto di queste scoperte è contenuto nel libro di Damasio, al cui interno sono narrate le vicende di Elliot, pseudonimo di un suo giovane paziente di circa trent'anni definito "novello *Phineas Gage*", la cui personalità aveva subito un decisivo cambiamento a seguito di un tumore al cervello che cresceva nell'area mediana del cranio e spingeva dal basso verso l'alto entrambi i lobi frontali, andando a causare lesioni alla corteccia prefrontale (regione della corteccia cerebrale responsabile dei processi di pianificazione, di decisione e anche di aspetti della personalità)⁶³. Da quel momento la vita di Elliot era cambiata: era diventato talmente freddo e distaccato da far dire ad amici e familiari che "*Elliot non era più Elliot*"⁶⁴.

⁶³ Trattasi forse dell'infortunio sul lavoro più celebre della storia delle neuroscienze. Phineas Gage era il capomastro che ebbe il cranio trafitto da parte a parte da una sbarra di ferro del diametro di tre centimetri di acciaio mentre prendeva parte alla costruzione di una ferrovia nel Vermont nel 1848. "*Sopravvissuto miracolosamente all'accaduto, Gage mantenne intatte le capacità di ragionamento logico, ma mostrò presto un forte cambiamento nel carattere: da persona stimata e affidabile, diventò – secondo la descrizione del dottore che lo prese in cura – bizzarro, insolente, poco riguardoso nei confronti dei compagni (...), capriccioso e oscillante*". In "*L'errore di Cartesio*", Damasio riporta anche il caso di un suo paziente, "*secondo Phineas Gage*", cui diede il nome immaginario di Elliot, il quale, a seguito della rimozione di un tumore che aveva coinvolto i lobi frontali, aveva manifestato analoghe tendenze caratteriali nonché, come Phineas Gage, una pressoché nulla capacità di imparare dai propri errori (Damasio A.R., *L'errore di Cartesio. Emozione, ragione e cervello umano*, Adelphi, Milano, 1995, pp. 71 ss.).

⁶⁴ *Ivi* p. 36.

In questa vicenda, ha suscitato attenzione in Damasio il fatto che il paziente, oltre all'incapacità di provare emozioni, fosse incapace anche di assumere decisioni⁶⁵. Ciò che, soprattutto, ha colpito il neuroscienziato è stato il comportamento del paziente:

*“Lo visitai subito, e ne fui colpito: era una persona piacevole ed interessante, dotata di un fascino profondo ma controllata nelle sue emozioni. Mostrava una compostezza riguardosa e piena di tatto, appena contraddetta da un lieve sorriso ironico indicante una saggezza superiore e una blanda condiscendenza verso le follie del mondo: appariva freddo, distaccato, imperturbabile, anche nel discutere di vicende personali che avrebbero potuto metterlo in imbarazzo. A me venne fatto di pensare a George Sanders quando impersona Addison DeWitt nel film *Eva contro Eva*”⁶⁶.*

Il paziente non riusciva più a decidere, nonostante avesse mantenute intatte tutte le sue facoltà cognitive (aveva un quoziente intellettivo superiore alla media e continuava a totalizzare punteggi molto alti in tutti i test psicologici cui veniva sottoposto)⁶⁷.

⁶⁵ *Ivi* pp. 34 e ss.

⁶⁶ *Ivi* p. 72.

⁶⁷ Nel corso degli anni Novanta, Damasio e i suoi collaboratori hanno ricostruito virtualmente la dinamica dell'incidente sulla base dei fori di entrata e di uscita del cranio, perfettamente visibili e conservati e, grazie a testimonianze dell'epoca, hanno stabilito una correlazione tra scelta razionale ed emozioni. Le ricerche condotte da Damasio sono all'origine di una teoria sull'influenza dell'emozione sui processi decisionali. Damasio, H., Grabowski, T., Galaburda, A., Damasio, A., *The Return of Phineas Gage: Clues about the Brain from the Skull of famous Patient*, in *Science*, 1994.

Questa correlazione ha portato Damasio a ricavare la sua teoria celebre del “marcatore somatico”⁶⁸, ipotizzando la rilevanza delle emozioni nel processo decisionale⁶⁹.

L’incapacità di provare emozioni, quindi, aveva generato nel paziente una incapacità di assumere decisioni, di decidere tra diverse alternative valide.

Damasio scrive che “*sia in Gage sia in Elliot, le strutture lese erano quelle che sono necessarie perché il ragionamento culmini nella decisione*”⁷⁰.

A seguito di questi esperimenti condotti su Elliot, Damasio e il suo gruppo di lavoro hanno dimostrato l’importanza del ruolo delle emozioni nel processo decisionale⁷¹ e come esse svolgano una funzione di guida cognitiva. Inoltre, sono arrivati ad altre

⁶⁸ La teoria del marcatore somatico è una teoria complessa che si avvale di risultati clinici e che lo stesso Damasio ha ampliato in una versione che mira a rendere conto della coscienza fenomenologica. Il marcatore somatico è definibile come un segnale a livello corporeo, più o meno intenso, che ci permette di anticipare le emozioni che si proverebbero a seguito delle conseguenze delle nostre azioni. In pratica, i marcatori permettono di disporre di una scala di preferenze ancor prima di aver fatto valutazioni razionali delle opzioni. I meccanismi fisiologici scatenati da un’emozione grazie all’attivazione del sistema nervoso autonomo sono marcatori che illuminano le nostre decisioni “razionali”.

Per dare credito alla sua teoria, Damasio ha studiato il comportamento di persone che hanno subito danni alla corteccia orbitofrontale e ha notato che queste non mostrano quelle reazioni del sistema nervoso autonomo che normalmente si accompagnano a un’attivazione emotiva. Cfr. Damasio, A., *The Feeling of What Happens: Body and Emotion in the Making of Consciousness*, New York, Harvest edition, 1999.

⁶⁹ A. Farano, *L’obbedienza al diritto tra ragioni e cause*, p. 108, https://iris.luiss.it/retrieve/e163de42-e367-19c7-e053-6605fe0a8397/Farano_TCRS_2021.pdf, data ultima visualizzazione 30/10/2022.

⁷⁰ Damasio, A., *Descartes’ Error: Emotion, Reason, and the Human Brain*, New York, Putnam, 1994, traduzione di Mancaluso, F., *L’errore di Cartesio*, Milano, Adelphi, 1995, p. 78.

⁷¹ V. par. 2.3.

importanti scoperte sul tema interagendo con gli studi condotti dai già citati Kahneman e Tversky, relativi all'avversione alle perdite^{72,73}

Nel suo saggio⁷⁴ Damasio dimostra come le emozioni siano alla base del buon funzionamento della mente: se l'uomo perde la capacità emozionale non è in grado di essere ragionevole.

Appare quindi opportuno, giunti a questo punto, fornire una definizione di emozione, intesa come azione o movimento relativamente pubblico, visibile ad altri giacché si manifesta nel volto, nella voce o in comportamenti specifici⁷⁵.

Secondo Damasio le emozioni fanno parte di quei meccanismi di regolazione, destinati a preservare la stabilità interna di un organismo al variare delle condizioni interne o esterne e, ove se ne presenti l'occasione, anche ad incrementarne il livello di benessere⁷⁶.

Per analizzare i tentativi di studio dell'emozione su base scientifica, occorre riferirsi obbligatoriamente a Charles Darwin, il quale in "*Expression of the emotions in man and animals*" del 1872⁷⁷, intendeva l'emozione come fenomeno espressivo legato alla

⁷² Kahneman, D., Tversky, A., *Prospect Theory: An Analysis of Decision under Risk*, in *Econometrica*, 47, 1979, pp. 111-132.

⁷³ Farano, A., *Emozioni e teoria del giudizio: una prima ricostruzione*, *BioLaw Journal*, *Rivista Di BioDiritto*, 2020, pp. 431-440, <https://doi.org/10.15168/2284-4503-535>, data ultima visualizzazione 31/10/2022.

⁷⁴ Damasio, A., *Descartes' Error: Emotion, Reason, and the Human Brain*, New York, Putnam, 1994, traduzione di Mancaluso, F., *L'errore di Cartesio*, Milano, Adelphi, 1995.

⁷⁵ Damasio, A., *Alla ricerca di Spinoza*, Adelphi, Milano, 2003, p. 252.

⁷⁶ Portera, M., *Spinoza "protobiologo"*, *Emozioni e sentimenti secondo Antonio Damasio*, rivista online del Seminario Permanente di Estetica, vol. 1, n. 1, p. 51, <https://doi.org/10.13128/Aisthesis-10935>, data ultima visualizzazione 30/10/2022.

⁷⁷ Darwin, C., *The Expression of the Emotions in Man and Animals*, Penguin Classics, 2005.

modificazione corporea sviluppata a seguito di un determinato stimolo ambientale⁷⁸. Secondo il suo pensiero, quindi, alcuni stimoli sarebbero in grado di attivare il sistema nervoso e indurre espressioni facciali e modifiche somatiche stereotipate che accomunano i diversi membri di una stessa specie.

In pratica, le emozioni sarebbero manifestazioni legate a una modificazione corporea funzionale all'azione da intraprendere in risposta a uno stimolo, ed espressioni atte a comunicare qualcosa⁷⁹.

Le emozioni svolgono un ruolo epistemico fondamentale poiché servono a richiamare l'attenzione, non solo su certi elementi di dettaglio essenziali della situazione, ma anche sulle stesse sensazioni vissute. Ci motivano, infatti, a cercare ragioni e prove che giustificano la condizione psicologica⁸⁰.

⁷⁸ Chece, D. M., *La filosofia delle emozioni dal pragmatismo alle neuroscienze*, in "Ragion pratica, Rivista semestrale" 2/2021, p. 585 <https://www.rivisteweb.it/doi/10.1415/102329>.

⁷⁹ Caruana e Viola riportano al riguardo la tesi della doppia evoluzione delle espressioni comportamentali introdotta dal filosofo Paul Griffiths, il quale sostiene che Darwin intendesse che *“certe espressioni comportamentali sono quello che sono perché si sono evolute due volte: una prima volta per fini adattivi; ma una seconda volta per propositi alquanto diversi: molte di queste espressioni sono state mantenute perché hanno acquisito, come nuova funzione, quella di regolare la comunicazione intraspecifica”*. Cfr. Griffiths 2003; Caruana, F., Viola, M., *Come funzionano le emozioni*, Il Mulino, Bologna, 2018.

⁸⁰ Forza, A., Menegon, G., Rumiati, R., *Il giudice emotivo. La decisione tra ragione ed emozione*, Il Mulino, Bologna, 2011, p. 60.

2.2 Anatomia e fisiologia delle emozioni

Damasio tratteggia una “fisiologia dell’emozione”, cercando di localizzare i siti del sistema nervoso centrale maggiormente implicati nello svolgimento dei fenomeni emozionali.

Il processo emotivo inizia quando un cervello sano rileva uno stimolo, cioè quando riesce a valutare un evento in grado di scatenare un’emozione.

In questa fase, chiamata “stadio della presentazione”, lo stimolo è presente alla mente. Da qui particolari segnali neurali passano a siti di induzione delle emozioni, nello specifico l’amigdala, situata in profondità nel lobo temporale, la corteccia prefrontale ventromediale e il cingolato.

Successivamente, vengono interessati i cosiddetti siti di esecuzione, cioè l’ipotalamo, il prosencefalo basale e alcuni nuclei del tegmento mesencefalico, i quali liberano una serie di sostanze chimiche nel sangue e inviano segnali neurali responsabili del cambiamento temporaneo della configurazione corporea.

Tutte quelle espressioni facciali e posture del corpo, che costituiscono la “fenomenologia” delle varie emozioni, sono l’esito di questo processo, lungo e complicato⁸¹.

A cosa servono però le emozioni? A questa domanda ha fornito una risposta convincente Daniel Goleman in *“L’intelligenza emotiva”* del 1995.

Quando incorriamo in situazioni troppo importanti per essere affidate al solo intelletto veniamo “aiutati” dalle emozioni che ci guidano nell’affrontare questi compiti. Ogni emozione ci orienta in una direzione già rivelatasi proficua nel ripetersi delle situazioni infinite della nostra storia evolutiva:

“Il valore del nostro repertorio emozionale ai fini della sopravvivenza trova conferma nel suo imprimersi nel nostro sistema nervoso come bagaglio

⁸¹ Ivi pp. 52-53.

comportamentale innato: in altre parole, nel fatto che le emozioni finiscono per diventare tendenze automatiche del nostro cuore [...] la stessa denominazione della nostra specie, Homo sapiens - la specie in grado di pensare - è fuorviante quando la si consideri alla luce delle nuove prospettive che la scienza ci offre per valutare il ruolo delle emozioni nella nostra vita. Come tutti sappiamo per esperienza personale, quando è il momento che decisione e azione prendano forma, i sentimenti contano almeno quanto il pensiero razionale, e spesso anche di più”⁸².

Ogni emozione è diversa e ha un ruolo preciso. Se abbiamo paura, il sangue affluisce verso i muscoli delle gambe, rendendo così più facile la fuga. Se siamo arrabbiati, il sangue affluisce alle mani e ciò rende più facile afferrare un’arma. Se, invece, siamo sorpresi solleviamo automaticamente le sopracciglia per avere così, una visione più ampia e per acquisire informazioni davanti ad una situazione non attesa. Il disgusto porta ad arricciare il naso, a chiudere le narici se sentiamo un odore nauseabondo. La tristezza comporta un crollo delle energie. Goleman ritiene che questo crollo fosse alle origini funzionale a trattenere gli esseri umani primordiali più vicini ai loro rifugi e, quindi, al sicuro dai pericoli, perché la loro condizione di tristezza li avrebbe resi più vulnerabili. Al contrario, la gioia porta ad una maggiore attività di un centro cerebrale che inibisce i sentimenti negativi e aumenta la disponibilità di energia⁸³.

⁸² Goleman, D., *L’intelligenza emotiva. Che cos’è e perché può renderci felici*, Rizzoli, Milano, 1995, p. 20.

⁸³ Forza, A., Menegon, G., Rumiati, R., *Il giudice emotivo. La decisione tra ragione ed emozione*, Il Mulino, Bologna, 2011, pp. 58-59.

2.3 Ruolo delle emozioni nella teoria giuridica

Nella tradizione filosofica occidentale, emozione e ragione sono sempre state considerate in antitesi tra loro. Questo contrasto portava a ritenere che *“quanto più si riesce a essere liberi dall’influenza delle emozioni, tanto più si può aspirare a condotte razionali”*⁸⁴.

Per questo motivo, per molto tempo⁸⁵ le emozioni sono state escluse dall’analisi dei processi decisionali in quanto considerate come fonte di disturbo nello svolgimento razionale del giudizio.

Nel diritto penale, il soggetto colpevole è un soggetto razionale, autonomo, che compie delle scelte effettuate liberamente sulla base di determinate capacità e sulla base della c.d. *“fair opportunity to do otherwise”*⁸⁶.

Il soggetto razionale si ritiene tale quando ha la capacità di intendere e di volere, per cui questo suo agire razionale è sorretto da due capacità: la capacità di comprensione e la capacità di controllo dei propri impulsi.

In questa visione razionalistica del comportamento, le emozioni non hanno molto spazio⁸⁷.

Il diritto penale effettua una separazione netta tra cognizione (base della razionalità) ed emozioni. La dottrina è pertanto concorde nell’affermare che il diritto penale adotti una concezione meccanicistica delle emozioni, come afferma anche Martha

⁸⁴ *Ivi*, p. 25.

⁸⁵ Fino agli anni Cinquanta, lo studio sui meccanismi mentali che controllano le decisioni era incentrato su regole di carattere razionale.

⁸⁶ Opportunità situazionale di poter agire diversamente.

⁸⁷ Anche nel nostro linguaggio comune, quando parliamo di una persona irrazionale ci riferiamo ad una persona emotiva, incapace di contenere le proprie emozioni.

Nussbaum⁸⁸, pioniera nella filosofia delle emozioni e grande pensatrice nel campo dell'etica, la quale basandosi anche su una tradizione filosofica razionalista, sostiene che il diritto penale abbia adottato una visione delle emozioni come stati mentali che non influiscono sulla razionalità in alcun modo positivo, ma sono degli elementi di disturbo del pensiero razionale.

A mettere in discussione la razionalità di alcune decisioni, sono stati alcuni scienziati cognitivi che da tempo si interrogavano sui reali fattori che stavano alla base delle scelte degli individui in campo economico e organizzativo.

Da qui è iniziato lo studio sulle modalità di adozione delle decisioni con un approccio descrittivo, verificando, tramite fattori che le determinano, come gli individui le prendono.

“Se le neuroscienze assumono come obiettivo quello di spiegare scientificamente il comportamento dell'uomo, individuando le cause cerebrali dello stesso, è evidente che il diritto in quanto tecnica di condizionamento del comportamento sia inevitabilmente esposto al dialogo con le neuroscienze”⁸⁹.

La funzione delle emozioni nelle scienze giuridiche non ha mai riscosso notevole rilevanza; ciò fin da subito è stato ritenuto essere un grande limite, soprattutto in

⁸⁸ Filosofa statunitense tra le più importanti del Novecento, i suoi studi sono stati improntati alla rivendicazione del ruolo sociale, politico e anche giuridico delle emozioni. Insegna *Law and Ethics* all'Università di Chicago, tra le sue opere principali si ricordano *“Diventare persone”* (2001), *“Giustizia sociale e dignità umana”* (2002), *“L'intelligenza delle emozioni”* (2009), *“La fragilità del bene”* (2011), *“Non per profitto”* (2013), *“Emozioni politiche”* (2014), *“Rabbia e perdono. La generosità come giustizia”* (2017).

⁸⁹ Owen Jones, 2013.

ambito penale dove sono spesso le emozioni a guidare il comportamento degli autori di reati⁹⁰.

L'ostacolo maggiore da superare per condividere l'impatto che le neuroscienze hanno nel campo giuridico è il riconoscimento di un legame inscindibile tra mente e corpo.

Tra i meriti delle neuroscienze è da annoverare la capacità di spiegare il rapporto tra la mente e le rappresentazioni esterne, cioè tra emozioni e decisioni, oltre alle opportunità che possono offrire alla formulazione dei giudizi.

Non mancano, tuttavia, posizioni contrarie di scettici, i quali ritengono che l'uso di strumenti neuroscientifici in sede processuale porterebbe un totale asservimento del processo decisionale alle prove scientifiche, andando così ad annullare il ruolo degli altri mezzi di prova. In questa maniera, quindi, l'unico giudice diventerebbe la prova scientifica⁹¹.

Al contrario, i sostenitori delle neuroscienze ritengono che i mezzi di prova neuroscientifici non renderebbero inutili le conoscenze pregresse, ma offrirebbero riscontri probatori *ad adiuvandum* per il giudice⁹².

Ne "*L'amore in Tribunale*", opera del giudice Lino Ferriani, viene identificata la figura del giurista in colui che per far risplendere "il sole della giustizia" deve essere in grado

⁹⁰ Cfr. Bodei, R., *Geometria delle passioni*, cit., pp. 9-14.

⁹¹ L'indagine sulla personalità del reo è stata storicamente messa da parte, questo a causa del rischio di un etichettamento arbitrario del reo, suscettibile di divenire per tal via bersaglio di un uso persecutorio o stigmatizzante del diritto penale. Il ricorso a neurotecniche e genetica comportamentale, inoltre, sposta l'accento sulla persona, mentre il nostro diritto penale è – al contrario – un diritto penale del fatto. Un'altra criticità potrebbe giacere nel rischio di un generalizzato giustificazionismo (per un'analisi approfondita, si veda Di Giovine O., *Ripensare il diritto penale attraverso le (neuro-)scienze?*, Giappichelli, Torino, 2020, pp. 57 ss.).

⁹² Flick, G. M., *Neuroscienze (diritto penale)*, rivista n. 4/2014, in *Enciclopedia Italiana di Scienze, Lettere ed Arti*, Nona appendice, Istituto dell'Enciclopedia Italiana, Roma, p. 2.

di distinguere tra passioni cieche e passioni ragionatrici, perché se l'amore può da un lato essere il più alto dei sentimenti, dall'altro più trasformarsi in una farsa⁹³.

La relazione che intercorre tra emozioni e diritto, sia in ambito civile che penale, non è facile da inquadrare nella teoria giuridica dal momento in cui le emozioni in tale ambito non sono considerate determinanti.

Nel corso degli ultimi anni, un gruppo di teorici del diritto ha cercato di chiarire il rapporto tra emozione e azione razionale attraverso una revisione della teoria scientifica sulle emozioni.

Facendo un breve *excursus* storico, è possibile rilevare, già nel IV secolo a.C. con il sistema di Aristotele, un preciso *discrimen* tra passioni ed emozioni: le prime sarebbero “*vere emozioni accompagnate da piacere o dispiacere*”, le seconde “*azioni sotto l'influenza delle passioni che possono possedere una chiara conoscenza della realtà*”⁹⁴.

Le teorie giuridiche volte a differenziare questi concetti hanno trovato un riscontro pratico alla luce di quanto sancito nell'art. 90 c.p., secondo il quale “*gli stati emotivi o passionali non escludono né diminuiscono l'imputabilità*”. È questa una norma molto controversa che nell'ordinamento penale, ha visto il legislatore impegnato, fin dal 1930, a disquisire nel merito, fino ad arrivare poi ad escludere la rilevanza degli stati emotivi e passionali in materia di imputabilità. Nonostante questa norma venga considerata, da larga parte della dottrina, di vana utilità, si coglie comunque un preciso intento del legislatore, cioè quello di evitare che possa essere considerato non punibile qualunque delitto impulsivo, indipendentemente da uno stato di menomazione della lucidità del soggetto agente.

⁹³ Ferriani, L., *Tra un processo e l'altro. L'amore in Tribunale*, cit., p. 170.

⁹⁴ Ferracuti, G., *Stati emotivi e passionali*, in Enc. dir., XLIII, Milano, 1990, p. 661.

Orientamenti minoritari ne negano qualsivoglia rilevanza sul piano giuridico, affermando che l'uomo “*deve saper resistere alle passioni*”⁹⁵, nonostante riconoscano che la psiche possa influenzare gli stati emotivi e passionali. Questa teoria è stata accolta in diverse sentenze della Suprema Corte⁹⁶.

Tuttavia, un orientamento sempre più consolidato⁹⁷ ritiene che uno sconvolgimento psicologico possa essere, di base, scaturito da uno stato passionale o emotivo e possa quindi essere equiparato all'infermità. Questa visione porta alla teorizzazione di una soluzione che oltrepassi quanto stabilito nell'art. 90 c.p., per dare spazio a stati psicologici che possano, eccezionalmente, generare “devianze”.

Questa è la visione ad oggi prevalente e paragona questi stati emotivi all'infermità mentale⁹⁸.

⁹⁵ Carnelutti, F., *Il problema penale della passione*, in Jus, 1954, p. 15.

⁹⁶ Cass., sez. I, 3 marzo 1993; Cass. sez. I 11 ottobre 1995 in CED Cassazione n 203651; Cass., sez. I, 22 aprile 1997; Cass. sez. I 5 dicembre 1997, in Cass. Pen., 1999, p. 156 in Riv. it. Med. Leg., 1999 p. 341 in CED Cassazione n. 209382.

⁹⁷ Di Dedda, E., *Gli stati emotivi e passionali come cause generative di infermità mentale*, in Nuovo Dir. 1934, p. 553, il quale specifica che un'emozione o una passione possono provocare in una persona normalmente equilibrata un turbamento tale da non “*porlo nella condizione anormale di colui che è incapace di volere*”, pertanto, anche se la legge esclude la rilevanza giuridica degli stati emotivi e passionali, in sé considerati, non esclude “*valore agli stati d'infermità transeunte derivante da emozioni o passioni*”; in senso conforme Madia, *Stati emotivi e passionali*, con riferimento all'art. 90, in Riv. dir. penit., 1957, p. 157.

⁹⁸ “*Stato mentale patologico che incide sulla capacità di intendere e di volere: tale infermità comporta l'esclusione della capacità di intendere e di volere, e dunque l'imputabilità, se il vizio di mente è totale (art. 88 c.p.), mentre comporta una ridotta capacità di intendere di volere se il vizio è parziale; in questo ultimo caso il soggetto risponde del reato commesso, ma la sua pena è diminuita (art. 89 c.p.). L'infermità psichica non coincide con il vizio totale di mente: i disturbi psichici possono escludere la capacità mentale del soggetto anche solo temporaneamente. L'infermità psichica condiziona l'attuazione della prognosi di pericolosità sociale*”, in Brocardi.it, <https://www.brocardi.it/dizionario/5766.html> , data ultima visualizzazione 15/02/2023.

Un ulteriore orientamento, fondato sul principio di colpevolezza, è stato portato avanti da illustri teorici⁹⁹ secondo i quali il legislatore degli anni '30 non esclude che gli stati emotivi incidano sull'elemento soggettivo fino ad eliminarlo, ma aggiungono che rimane impregiudicata la questione della responsabilità dell'agente¹⁰⁰.

Ad oggi la Suprema Corte riconosce gli stati emotivi e passionali *“come un vero e proprio squilibrio mentale che comporta la totale perdita dei freni inibitori e della volontà”*¹⁰¹. Si tratta, quindi, di una patologia che determina, seppur in via transitoria, uno stato di non punibilità che considera ogni condotta turbata da situazioni di stati emotivi e passionali meritevoli di accertamento giudiziale, anche tramite strumenti neuroscientifici che evidenzino il nesso sociologico tra patologia psichiatrica e condotte compromissive del normale stato psicologico del soggetto agente.

Possiamo concludere affermando che, in assenza di una definizione uniforme, gli stati emotivi e passionali, nonostante i vari tentativi portati avanti in campo scientifico, risultano ancora un'incognita che la giurisprudenza deve risolvere di volta in volta.

2.3.1 La forza delle emozioni nel processo

Nel nostro ordinamento, la Corte di cassazione rappresenta l'ultimo grado di giudizio.

Di regola, è chiamata a decidere riguardo i ricorsi contro le sentenze d'appello.

I giudici d'appello, quelli cioè di secondo grado, si occupano delle decisioni di primo grado, entrano nel merito dei fatti del singolo caso e, se necessario, rivalutano le prove.

⁹⁹ De Vincentiis, P., L'art. 90 del Codice penale, in Giust. pen., 1947 per il quale gli stati emotivi e passionali possono non incidere per nulla sull'attività psichica o incidere fino a tal punto da provocare un'infermità mentale vera e propria. Di conseguenza l'art. 90 c.p., contenendo una presunzione di impossibilità che gli stati emotivi e passionali diano luogo a malattie mentali, andrebbe eliminato, invocandosi addirittura il riconoscimento legislativo di un nuovo delinquente: quello passionale.

¹⁰⁰ V. Santacroce, *Stati emotivi o passionali e nesso psichico*, in Giur. merito., 1974, II, p. 301.

¹⁰¹ Cass., sez. V, 5 aprile 1990, in Cass. pen., 1991, I, p. 1565.

Tutto ciò è precluso ai magistrati della suprema corte, in quanto il perimetro delle loro decisioni è circoscritto alle questioni di diritto e ai vizi logici della motivazione.

Quanto, quindi, possono influire le emozioni sul processo decisionale dei supremi giudici?

Abbiamo detto che una sentenza del Tribunale può essere appellata avanti la Corte d'appello. Così, il giudice di secondo grado entra nuovamente nel merito della vicenda processuale, riesamina i fatti, riconsidera le prove e, se occorre, ne ammette di nuove.

La Corte di cassazione, invece, vede limitato il proprio intervento ad una valutazione delle questioni di legittimità poste dal ricorso. In pratica, il suo compito è quello di stabilire se i giudici di secondo grado abbiano applicato le norme correttamente.

Perciò, se la sentenza dei giudici d'appello è viziata da errori di diritto, la Corte provvede ad annullarla e a rinviarla ad altra sezione della stessa Corte d'appello, la quale nuovamente, si pronuncia nel merito, applicando il principio di diritto stabilito dalla Suprema corte.

Giunti a questo punto, dovremmo ritenere che questa tipologia di magistrato, lontano da fatti, prove e persone, sia interessato alle sole questioni di diritto, senza alcun coinvolgimento emotivo. Non risulta, però, essere così, da quello che si evince nelle parole di Altavilla:

“Il magistrato di Cassazione risente naturalmente dei difetti dell'istituto di cui è espressione. Per quanto andai dicendo, il giudizio di merito si risolve non raramente in una mostruosità logica ed etica che il magistrato spesso corregge, con scandalo dei giuristi puri, trasformandosi in un giudice di fatto.

Il fatto e il diritto, l'uomo e il delitto sono così intimamente connessi che ogni scissione si risolve in un'anomalia, a ciò si aggiunga che il diritto deve avere una funzione sociale ed etica, ora la sua scissione dal fatto turba alle volte questa sua funzione, ciò sente il magistrato e tortura la legge nell'interesse dell'etica.

*Quanti imputati di un turpe reato hanno visto respinto un ricorso fondato su gravi motivi, e quanti ricorsi insostenibili sono stati accolti, perché si è voluto dare mezzo al magistrato di rinvio di correggere un'ingiustizia*¹⁰².

Le emozioni suscitate dalla vicenda umana, dunque, colpiscono anche i magistrati di Cassazione in pari misura e, forse, più dei giudici di merito. Più sono numerose le ombre sui fatti e più trovano spazio le convinzioni personali su come possano essersi svolti quei fatti stessi. Anche il più tecnico dei ricorsi è destinato ad entrare inevitabilmente nell'ambito della fattispecie concreta a suscitare emozioni.

Gli aspetti del fatto, che sembrano essere marginali nel giudizio di legittimità, sono di per sé atti ad influenzare non solo la soluzione del problema giuridico, ma l'intero processo di ragionamento.

In sintesi, anche i magistrati di ultima istanza, come ognuno di noi, non decidono in condizioni emotivamente neutre, ma sulla base della valutazione degli eventi associata alla componente affettiva, nonostante operino in condizioni di stress temporale e decidano in tempi ristretti¹⁰³.

¹⁰² Altavilla, E., *Psicologia giudiziaria*, Torino, Unione Tipografico-Editrice Torinese, 1948, p. 768.

¹⁰³ "Lo psicologo del comportamento Dylan Evans, in un suo recente lavoro, cita un passo significativo del filosofo inglese John Locke, tratto dal Saggio sull'intelligenza umana. Come «per la maggior parte di ciò che ci interessa, [Dio] ci ha concesso solo il crepuscolo, così si potrebbe dire della probabilità» [Locke 1690, 745]. Qual è il messaggio, antico di quattro secoli, che si può ricavare da questa citazione? Quali esseri umani non siamo equipaggiati per operare in questa zona crepuscolare. Se siamo corretti, non osiamo azzardare un'opinione su cose di cui abbiamo, in realtà, solo una vaga idea. Se siamo troppo sicuri di noi stessi, facciamo l'esatto contrario e cioè azzardiamo opinioni su cose che si trovano nella zona crepuscolare. Per usare l'immagine della stanza buia, altrettanto evocativa, proposta da Evans, la decisione in condizioni di incertezza viene assunta quando la conoscenza delle informazioni necessarie è limitata. È come se la mente del decisore si trovasse al centro di una stanza

Questo perché anche i giudici sono persone, quindi è inevitabile che il meccanismo che scatta nella loro mente di essere umano è quella reazione “affettiva” inconsapevole che finisce per condizionarli comunque.

In conclusione, quindi, il giudizio finale è, la maggior parte delle volte, influenzato dall’elaborazione emotiva e dalla selezione stessa delle informazioni che il carattere affettivo determina, anche inconsciamente¹⁰⁴.

2.3.1.1 “Justice is what the judge ate for breakfast”

Nel 2011, alla *Columbia University*, è stato condotto uno studio (con sorprendenti risultati raggiunti) da tre ricercatori¹⁰⁵, in collaborazione con L’Università di Tel Aviv, successivamente pubblicato sulla rivista scientifica *PNAS*¹⁰⁶, con lo scopo di testare una battuta caricaturale della prospettiva realista¹⁰⁷, pronunciata in un saggio degli anni Novanta dello scorso secolo, che aveva fatto molto discutere. Questa caricatura della prospettiva realista si può concentrare nell’aforisma *justice is what the judge ate for breakfast* (la giustizia è quello che il giudice ha mangiato a colazione).

*illuminata dalla luce fioca di una sola lampadina. Egli potrà tener conto delle cose più vicine e illuminate che può vedere, mentre altre, magari più importanti, restano nell'oscurità. Potrà sopporle, potrà inferire la loro presenza ma in tali condizioni, appunto, di limitata conoscenza, ogni presa di decisione è assoggettata a rischio [Evans 2012].” Cfr. Forza, A., Menegon, G., Rumiati, R., *Il giudice emotivo. La decisione tra ragione ed emozione*, Il Mulino, Bologna, 2011, pp. 89-90*

¹⁰⁴ *Ivi* 86-89.

¹⁰⁵ Danziger, Levav e Avnaim-Pesso.

¹⁰⁶ <https://www.pnas.org/doi/epdf/10.1073/pnas.1018033108>, data ultima visualizzazione 16/11/2022.

¹⁰⁷ Il “realismo giuridico” è andato ad affermarsi nel periodo compreso tra la fine degli anni Venti e la fine degli anni Trenta del secolo scorso negli Stati Uniti. Questa corrente avversava fermamente la tesi formalista, fino a quel momento dominante nella filosofia del diritto, che riconduceva il ragionamento giuridico alla sola logica dimostrativa. Il realismo americano ha avuto un impatto considerevole sulla teoria del diritto, con una visione diversa circa i processi di formazione della decisione giudiziale.

I ricercatori hanno esaminato le conclusioni di 1100 sentenze emesse, in sequenza, da otto giudici di due distinti Tribunali israeliani, competenti a decidere se concedere o meno la libertà per buona condotta ai detenuti delle quattro carceri più grandi del paese.

Dai risultati è emerso che le decisioni di accoglimento dei benefici richiesti dai condannati diminuiscono del 65% se assunte lontano dalle pause. Nella sequenza dei casi, quindi, la probabilità di una sentenza favorevole è maggiore all'inizio della giornata lavorativa o dopo una pausa, piuttosto che più tardi.

Questa indagine è stata effettuata sulla base del lavoro di una serie di giudici, per un periodo di tempo di 10 mesi, durante i quali ciascuno di essi ha trattato dai 14 ai 35 casi.

Durante le giornate i giudici hanno svolto tre sessioni di lavoro, interrotte da due pause, una per il caffè e una per il pranzo (con durate e orari variabili). Così è stato possibile verificare il loro effetto sul giudicante.

I risultati a cui sono giunti i ricercatori hanno dimostrato che la tendenza ad emettere una sentenza favorevole per il detenuto è maggiore all'inizio di ogni sessione di lavoro, mentre si riduce via via che ci si avvicina alla sessione successiva.

Nelle scelte dei giudici, dunque, hanno assunto rilevanza fattori totalmente avulsi dalle questioni giuridiche trattate.

È quindi evidente, secondo questo esperimento, che le ragioni di tali risultati vanno ricercate in ambiti diversi da quelli del diritto, come la psicobiologia del cervello e la fisiologia del corpo umano.

Un lavoro ripetitivo, come la routine cui sono sottoposti giudici in questo caso, esaurisce le risorse mentali del soggetto, lo porta ad aumentare la tendenza alla semplificazione dei problemi. Una buona *forma mentis* può essere ripristinata dopo una breve pausa e dopo aver aumentato i livelli di glucosio nel sangue, con l'assunzione di cibo o di una bevanda.

Questi risultati permettono di affermare che, anche nelle decisioni dove si deve stabilire la responsabilità di un imputato, la condizione psicofisica di chi giudica può assumere un valore determinante. Infatti, un giudice riposato giungerà a decisioni più meditate di uno stanco.

Naturalmente, vengono meno dati empirici per sostenere con convinzione quanto una pausa possa influire nel lavoro dei giudici, anche di quelli professionali nell'ambito di processi complessi. Permane, in ogni caso il dato indiscusso che variabili estranee alle questioni tecnico-giuridiche possano influenzare il processo decisorio anche per i giudici con lunga esperienza¹⁰⁸.

2.3.2 Neuroscienze e accertamento della responsabilità e dell'imputabilità; Sentenza Trieste

L'applicazione delle neuroscienze nel diritto ha rappresentato, negli ultimi anni, uno dei settori di studio di interesse rilevante in ambito giuridico.

Il compito principale delle neuroscienze è quello di comprendere come funziona il sistema nervoso¹⁰⁹. La branca di maggior interesse, in questa sede, è quella delle neuroscienze cognitive, che si occupa di studiare come le variazioni anatomiche o fisiologiche nel cervello possano influenzare il comportamento.

Le "neuroscienze giuridiche" costituiscono importanti aiuti nell'applicazione delle neuroscienze al diritto.

¹⁰⁸ Forza, A., Menegon, G., Rumiati, R., *Il giudice emotivo. La decisione tra ragione ed emozione*, Il Mulino, Bologna, 2011, pp. 123-126.

¹⁰⁹ Tra queste, possiamo citare, per esempio, la "neuro-economia", che si occupa dei processi decisionali che sono alla base delle scelte economiche, la "neuro-ingegneria", che sfrutta tecniche ingegneristiche al fine di migliorare le funzionalità del sistema nervoso, gli studi sull'Intelligenza Artificiale, che mirano a conferire ad un elaboratore l'abilità di effettuare ragionamenti tipici della mente umana.

È necessario in questo ambito iniziare con la lettura dei principi contenuti negli artt. 25 e 27 della Costituzione.

L'art. 25 sancisce che

“Nessuno può essere distolto dal giudice naturale precostituito per legge.

Nessuno può essere punito se non in forza di una legge che sia entrata in vigore prima del fatto commesso.

Nessuno può essere sottoposto a misure di sicurezza se non nei casi previsti dalla legge”¹¹⁰.

Siamo, qui, di fronte al principio di legalità in materia penale. Questa norma induce a rivalutare i corollari della riserva di legge e della tassatività. Con le nuove scoperte in campo neuroscientifico, è stato demistificato il dogma della certezza del diritto¹¹¹. Qui le neuroscienze non introducono in materia penale argomenti nuovi, ma avvalorano ipotesi già prospettate¹¹².

Un'altra norma della Costituzione che può essere letta attraverso gli apporti delle neuroscienze è l'art. 27 secondo cui

“La responsabilità penale è personale.

L'imputato non è considerato colpevole sino alla condanna definitiva.

Le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere alla rieducazione del condannato.

¹¹⁰ Costituzione Italiana, <https://www.senato.it/istituzione/la-costituzione/parte-i/titolo-i/articolo-25>.

¹¹¹ In un'ottica pienamente conforme a quanto già sostenuto nella nota sentenza della Corte Costituzionale n. 364 del 1998.

¹¹² Flick, G. M., *Neuroscienze (diritto penale)*, rivista n. 4/2014, in Enciclopedia Italiana di Scienze, Lettere ed Arti, Nona appendice, Istituto dell'Enciclopedia Italiana, Roma, p. 5.

*Non è ammessa la pena di morte*¹¹³.

Questa norma è fondamentale per la costruzione della responsabilità penale “personale” e, perciò, per tracciare i confini della colpevolezza.

In particolare, il tema affrontato è quello della colpa, soprattutto nella forma omissiva. In questo ambito il rilievo delle neuroscienze si rinviene in temi quali il “controllo doveroso” e la “possibilità di impedire l’evento”. È grazie ad esiti in campo neuroscientifico che sembra ormai indispensabile tenere conto di situazioni in cui vi siano anomalie psichiche e patologie della sfera emotiva, nei casi in cui si accerti la colpevolezza in senso psicologico¹¹⁴.

Una pronuncia del 2009 ha fatto ricorso diretto agli strumenti e alle scoperte messi a disposizione dalle neuroscienze. Si tratta di una sentenza della Corte d’Assise d’Appello di Trieste (n. 5/2009)¹¹⁵, che ha ridotto di un terzo la pena dell’imputato, condannato per omicidio, a seguito della attestazione di semi-infermità di mente, dichiarata dalla perizia condotta da due noti esperti¹¹⁶. Tale perizia si fonda sulla base

¹¹³ Costituzione Italiana, <https://www.senato.it/istituzione/la-costituzione/parte-i/titolo-i/articolo-27> .

¹¹⁴ *Ivi* pp. 5-6.

¹¹⁵ Nello specifico il quesito posto dal giudice riguardava la capacità di intendere e di volere al momento del fatto. A.B., uomo di 40 di origine algerina riferisce di essere entrato nell’esercito algerino come militare, dopo aver abbandonato gli studi, per poi iniziare a lavorare come muratore. Successivamente decide di trasferirsi in Italia. Un pomeriggio, tornando a casa – con gli occhi truccati per motivi religiosi, come era sua abitudine fare – nota una persona che lo sta fissando e gli rivolge gesti con intento provocatorio e di derisione, apostrofandolo come gay. Da qui nasce una discussione tra loro, degenerata poi con un’aggressione. Dopo di che, su suggerimento di un amico, A.B. si reca ad acquistare un coltello – che avrebbe nascosto sotto i vestiti – e, una volta tornato sul luogo della disputa, colpisce a morte un soggetto, simile per il colore della pelle, ma che non è colui che poco prima l’aveva offeso.

¹¹⁶ Si tratta di Giovanni Sartor, professore di neuroscienze cognitive e di neuropsicologia clinica all’Università di Padova, e di Pietro Pietrini, professore di Biochimica Clinica e Biologia Molecolare

dei dati provenienti dall'esame neuropsicologico¹¹⁷, dall'*imaging*¹¹⁸ funzionale e dalla genetica molecolare del comportamento del soggetto. È la prima volta che in Europa la genetica molecolare del comportamento riesce a influenzare una sentenza al punto da consentire una significativa riduzione di pena a un condannato per omicidio, sulla base di una perizia psichiatrica indipendente.

Clinica presso il dipartimento di patologia sperimentale, biotecnologie mediche, infettivologia ed epidemiologia dell'Università di Pisa. Cfr. Corte di Assise d'Appello di Trieste, R.G.N.R. 1685/2007, sent. 18 settembre 2009, n. 5.

¹¹⁷ Nel caso in questione, A.B., viene sottoposto ad un test della personalità dal quale emerge un profilo caratterizzato da insicurezza, bassa autostima e alternanza di maniacalità. Inoltre, viene rilevata la presenza di un disturbo del pensiero e un disturbo da delirio, elementi che conducono ad ipotizzare problematiche di tipo psicotico. Nel soggetto compaiono, poi, anomalie percettive come cambiamenti visivi, uditivi e somatici.

Per verificare l'effettiva capacità di bloccare l'azione e quindi della sussistenza dell'impulso irresistibile, la giurisprudenza anglosassone propone l'applicazione del test del "poliziotto con la pistola a fianco" il quale consiste nel chiedere all'imputato quale comportamento avrebbe tenuto in presenza di un poliziotto con la pistola. Se risponde che avrebbe comunque compiuto l'azione, andrebbe a indicare la presenza di un impulso talmente forte che nemmeno la presenza del poliziotto avrebbe potuto contrastarla e quindi l'autore del reato, in questo caso, non è in grado di inibire l'azione. A questa prova, A.B., fornisce risposta negativa, affermando che, in presenza del poliziotto, non avrebbe accoltellato l'uomo.

¹¹⁸ Le tecniche di neuroimaging (RM strutturale e funzionale, TAC, PET, ecc.) permettono di studiare l'encefalo e di individuare le aree che, se lesionate, possono provocare quei deficit cognitivi e comportamenti che compromettono la capacità di autodeterminazione. Cfr. Codognotto, S., Sartor, G., *Neuroscienze in tribunale: la sentenza di Trieste*, in "Sistemi intelligenti, Rivista quadrimestrale di scienze cognitive e di intelligenza artificiale" 2/2010, p. 275.

Questa sentenza riconosce efficacia probatoria alle neuroscienze cognitive¹¹⁹ e molecolari, segnalando come l'utilizzo di queste tecniche aumenti la certezza che ci si trovi di fronte ad una vera e propria infermità di mente¹²⁰.

Generalmente, sia il processo penale che quello civile si pongono come obiettivo quello di definire se una determinata azione sia il risultato di una libera scelta o se invece le azioni siano state “deviate” da fattori esterni alla volontà dell'individuo.

Quando un reato viene commesso da un soggetto privo di capacità di intendere o di volere a causa di una infermità di mente¹²¹ il soggetto non è imputabile per quel determinato reato¹²².

Bisogna, quindi, distinguere il “*Bad from Mad*”, in quanto solo il “cattivo” deve essere punito, non il “pazzo”, dal momento in cui solo il primo ha scelto di agire in un determinato modo mentre il libero arbitrio del secondo viene sostituito dalla malattia mentale¹²³.

Le recenti scoperte nel campo della genetica molecolare e delle neuroscienze, riguardanti i meccanismi cerebrali del comportamento criminale, hanno contribuito a procurare delle parziali risposte che non possono essere ignorate.

¹¹⁹ L'espressione “neuroscienze cognitive” si deve a Michael Gazzaniga, che ne fornisce la seguente definizione: “*cognitive neuroscientist attempt to discover the molecular logic of organic knowledge systems, i.e. the principles that, in addition to the principles of physics, chemistry, biology, and psychology, govern the behavior of inanimate matter in living knowledge systems*”. Gazzaniga, M.S. (a cura di), *Cognitive Neuroscience: A Reader*, Oxford, 2000, p. 11.

¹²⁰ Codognotto, S., Sartor, G., *Neuroscienze in tribunale: la sentenza di Trieste*, in "Sistemi intelligenti, Rivista quadrimestrale di scienze cognitive e di intelligenza artificiale" 2/2010, p. 269.

¹²¹ Concetto giuridico che si riferisce ma non corrisponde esattamente alla malattia mentale.

¹²² Cfr. art. 88 c.p. “*Non è imputabile chi, nel momento in cui ha commesso il fatto, era, per infermità, in tale stato di mente da escludere la capacità di intendere o di volere*”.

¹²³ Codognotto, S., Sartor, G., *Neuroscienze in tribunale: la sentenza di Trieste*, in "Sistemi intelligenti, Rivista quadrimestrale di scienze cognitive e di intelligenza artificiale" 2/2010, p. 270.

Ricapitolando, nel caso in questione è stato possibile provare un vizio parziale di mente¹²⁴, dimostrando che la capacità di intendere e di volere¹²⁵ è fortemente scemata a seguito di un'infermità di mente¹²⁶.

In conclusione, le conoscenze neuroscientifiche e genetiche consentono di superare i limiti di bassa oggettività derivanti dall'applicazione della valutazione psichiatrica forense tradizionale. Vi è, perciò, la necessità di accertamenti più obiettivi per facilitare la formulazione di un giudizio più imparziale e oggettivo. L'utilizzo, quindi, di strumenti di valutazione standardizzati è di aiuto nella formulazione diagnostica poiché riduce notevolmente il margine di discrezionalità della valutazione sulla capacità di intendere e di volere, pervenendo così alla formulazione di pareri utili a giudizi "oltre ogni ragionevole dubbio"¹²⁷.

¹²⁴ *"Ai fini del riconoscimento del vizio totale o parziale di mente, rientrano nel concetto di "infermità" anche i "gravi disturbi della personalità", a condizione che il giudice ne accerti la gravità e l'intensità, tali da escludere o scemare grandemente la capacità di intendere e di volere, e il nesso eziologico con la specifica azione criminosa".* Principio di diritto espresso da Cass. Sez. Un., 8 marzo 2005, n. 9163, Raso.

¹²⁵ Termine giuridico che indica la capacità di rendersi conto della realtà e del valore sociale delle proprie azioni – capacità di intendere – e quale attitudine ad autodeterminarsi esercitando il controllo su stimoli e reazioni – capacità di volere – (art. 85 c.p., art. 428 c.c.).

¹²⁶ Concetto interpretato dalla giurisprudenza come indicante un'alterazione patologica del sistema nervoso che incide sulla capacità di intendere e di volere. Tale infermità comporta l'esclusione della capacità di intendere e di volere e, dunque, l'imputabilità se il vizio di mente è totale (art. 88 c.p.), mentre comporta una ridotta capacità di intendere e di volere se il vizio è parziale; in quest'ultimo caso il soggetto risponde del reato commesso, ma la pena è diminuita (art. 89 c.p.).

¹²⁷ Ai sensi dell'art. 533 c.p., il giudice pronuncia sentenza di condanna se l'imputato risulta colpevole del reato "al di là di ogni ragionevole dubbio". Il riferimento al ragionevole dubbio è stato inserito con L. 46/2006 che stabilisce la necessità di un alto grado di probabilità di colpevolezza dell'imputato, non

2.3.3 (Segue) ... Ulteriori riferimenti giurisprudenziali sul tema dell'accertamento della responsabilità

a) Sentenza n. 536/2011 del Tribunale di Como

Un altro riferimento giurisprudenziale in materia lo troviamo nella sentenza n.536/2011 del Tribunale di Como.

Il caso in esame si riferisce a fatti avvenuti nel 2009 nella provincia di Como, quando Stefania Albertani uccide la sorella, segregandola in casa e costringendola ad assumere psicofarmaci in dosi tali da causarne il decesso, per poi dare fuoco al cadavere.

Successivamente, mentre è indiziata e tenuta sotto controllo dalla polizia per la scomparsa della sorella, durante un diverbio con la madre, tenta di strangolare quest'ultima con una cintura. L'arrivo tempestivo della polizia salva la madre e porta in arresto la Albertani.

In base al complesso disegno criminoso emerso, l'imputata viene chiamata a rispondere di sequestro di persona e dell'omicidio della sorella, nonché dei reati di soppressione e distruzione del cadavere, di utilizzo indebito delle carte di credito della sorella e di procurata incapacità di intendere e di volere del padre attraverso la somministrazione di medicinali che ne procurano il ricovero in ospedale, di tentato omicidio di entrambi i genitori – avendo cercato di far esplodere la loro vettura – e, infine, del tentato omicidio della madre tramite lo strangolamento.

La difesa dell'imputata chiede di procedere con rito abbreviato, tentando di far emergere fin da subito, la presenza di un vizio di mente della stessa. Vengono, quindi,

ritenendo sufficiente un minimo dubbio di colpevolezza per poter arrivare alla pronuncia di una sentenza di condanna.

Il giudice applica la pena discrezionalmente, indicandone i motivi. Tuttavia, il principio dell'oltre ogni ragionevole dubbio rappresenta un limite alla libertà di convincimento del giudice, al fine di evitare che la decisione finale venga presa in base ad apprezzamenti meramente soggettivi.

effettuate tre valutazioni da parte di esperti psichiatrici, risultate completamente differenti l'una dall'altra: la perizia richiesta dal giudice evidenzia una piena capacità di intendere e di volere, la consulenza tecnica del P.M. l'esistenza di un vizio parziale di mente e, infine, la consulenza tecnica della difesa diagnostica un vizio totale di mente.

A questo punto, il giudice altro non può che ammettere un'ulteriore prova richiesta dalla difesa (una perizia neuroscientifica in grado di rilevare la presenza di un vizio di mente con un maggior grado di oggettività). Con questa richiesta emerge un evidente disappunto nei confronti della psichiatria, non più capace di “distinguere con sicurezza e precisione tra sanità ed infermità mentale”¹²⁸. Si perviene, dunque, a metodologie fondate sull'evidenza dei dati come quelle “corroborate dalle risultanze dell'*imaging* cerebrale”¹²⁹.

La decisione circa l'imputabilità deve, quindi, risultare da una convergenza di indagini scientifiche e emergenze processuali, come cita lo stesso estensore della sentenza per cui “*una volta ottenuto l'esito della scienza psichiatrica che individua i requisiti biopsicologici di una eventuale anomalia mentale, resta al giudice il compito di valutare la rilevanza giuridica dei dati forniti dalla scienza ai fini della rimproverabilità dei fatti commessi al suo autore, sulla base del complesso delle risultanze processuali e sulla valutazione logica e coordinata di tutte le emergenze*”¹³⁰.

Il G.i.p. di Como, Luisa Lo Gatto, opta, in conclusione, per l'accoglimento della tesi dei consulenti della difesa poiché “oltre ad apparire il frutto di accertamenti più rigorosi e completi, rivelano piena aderenza alle emergenze processuali”¹³¹.

¹²⁸ Sentenza G.i.p. Como, 20 maggio 2011, cit. p.29.

¹²⁹ *Ivi*, p. 39.

¹³⁰ Sentenza G.i.p. Como, 20 maggio 2011, cit. p. 54.

¹³¹ *Ibidem*.

La Albertani viene condannata a vent'anni di reclusione, venendole riconosciuto un vizio parziale di mente per la presenza di alterazioni in un'area del cervello che ha la funzione di regolare le azioni aggressive e, dal punto di vista genetico, di fattori *“significativamente associati ad un maggior rischio di comportamento impulsivo, aggressivo e violento”*¹³².

Si tratta, pertanto, di un fondamentale riconoscimento in Italia¹³³, e uno fra i primi al mondo, della validità delle neuroscienze per l'accertamento dell'imputabilità.

La sentenza segna un'importante apertura al contributo delle nuove tecniche di indagine offerte dalle neuroscienze alla valutazione della capacità di intendere e di volere dell'imputato nel processo penale.

b) Sentenza n. 296/2013 del Tribunale di Venezia

Si cita di seguito ulteriormente il noto caso Mattiello, relativo ad un'infausta vicenda di cronaca, in cui sono state utilizzate conoscenze neuroscientifiche per l'emissione di un giudizio circa la capacità di intendere e di volere dell'imputato.

Un pediatra di Vicenza, il dott. Mattiello viene ritenuto colpevole di abusi sessuali su minori per aver molestato, durante le visite mediche in un asilo¹³⁴, alcune bambine¹³⁵.

Il lavoro del giudice, in questa vicenda, consiste nel verificare la corretta capacità di intendere e di volere dell'imputato. Infatti, durante il procedimento al dott. Mattiello,

¹³² G.i.p. Como, 20 maggio 2011, in Guida al diritto (on line), 30 agosto 2011, con nota di Maciocchi P., G.i.p. di Como: le neuroscienze entrano e vincono in tribunale.

¹³³ Insieme al precedente giurisprudenziale di cui al paragrafo precedente.

¹³⁴ Circostanza che assume rilievo nella decisione è che il pediatra commette atti di pedofilia sono in uno degli asili frequentati, quello in cui i bambini vengono lasciati soli con il medico durante le visite.

¹³⁵ Tribunale di Venezia, G.i.p. dott.ssa Roberta Marchiori, 24 gennaio-8 aprile 2013, sent. n. 296.

sottoposto a risonanza magnetica funzionale, viene riscontrato un tumore al cervello (cordoma del clivus), successivamente asportato in due differenti interventi.

La relazione dei consulenti di parte, i noti proff. Sartor e Pertini¹³⁶, prodotta con l'ausilio delle risultanze neuroscientifiche, afferma che l'imputabilità del soggetto non rileva, anche se questo avviene sulla base di uno studio diverso rispetto a quello relativo alle vicende processuali di Como e Trieste. In questa fattispecie, infatti, la patologia riscontrata è stata individuata quale causa esclusiva del mutato orientamento sessuale del medico, tale da ingenerare in lui l'irresistibile impulso di abusare delle giovani vittime. Il caso in esame è, quindi, solo in parte sovrapponibile a quelli precedenti, in quanto coinvolge principalmente il parametro normativo della capacità di volere e impone una riflessione sul nesso tra identità e responsabilità che la teoria del carattere sembra in parte attivare¹³⁷.¹³⁸

L'esito dei test neuropsicologici, come si evince dalla perizia, rivela una piena capacità di intendere combinata, tuttavia, ad alcuni dati fuori norma: viene riscontrata un'incapacità di riconoscere le espressioni idiomatiche, debolezze interpretate alla stregua di "*tipici marker di compressione frontale*"¹³⁹. A ciò, si aggiungono ulteriori deficit delle funzioni frontali, quali "*capacità attentive, di recupero di parole su accesso fonemico, di riconoscimento dei contorni, distinzione figura-sfondo, segmentazione delle figure o esplorazione spaziale*"¹⁴⁰.

¹³⁶ Rilevanti nei casi precedentemente citati (v. par. 2.3.2 a, b): Corte d'Assise d'Appello di Trieste, n. 5/2009, e Tribunale di Como, G.i.p., 20 maggio- 20 agosto 2011.

¹³⁷ Si ricorda che il processo di primo grado si conclude con il rigetto della consulenza di parte e la condanna dell'imputato a cinque anni di reclusione (condanna confermata in appello, con la riduzione tuttavia della pena di circa la metà).

¹³⁸ Farano, A., *La responsabilità giuridica alla prova delle neuroscienze*, Bari, Cacucci Editore, 2018, p. 158.

¹³⁹ Sentenza del Tribunale di Venezia, G.i.p. dott.ssa Marchiori, 24 gennaio-8 aprile 2013, n. 296, p. 13.

¹⁴⁰ *Ibidem*.

Nella valutazione delle capacità del paziente, i periti rilevano, inoltre, una “difficoltà nella inibizione di comportamenti automatici” che assumerebbero un ruolo primario “*nella criminogenetica, laddove la compulsione ad agire può trovare freno nei meccanismi inibitori alterati*”¹⁴¹.

Dopo aver descritto i sintomi, i periti somministrano all'imputato il test a-IAT (*autobiographical implicit association test*), ideato da Tony Greenwald¹⁴², che permette di verificare la presenza di tracce mnestiche affidabili mediante monitoraggio. In questo caso, l'affermazione del pediatra di aver iniziato ad avere un orientamento sessuale deviato solo un anno prima del processo – in concomitanza con l'insorgere del tumore – sarebbe vera.

Il tumore potrebbe aver determinato il comportamento del dott. Mattiello in più modi. “*comprimendo le strutture della corteccia orbito facciale mediale, data la prossimità della sella turcica alla stessa; provocando disfunzioni delle strutture sottocorticali connesse alla corteccia orbitofrontale (ipotalamo, ipofisi); comprimendo le fibre nervose di connessione cortico sottocorticali e cortico ponto cerebellari che passano nel tronco dell'encefalo e nel ponte (peduncoli cerebellari)*”¹⁴³.

Il quadro clinico a cui giungono i periti riferisce di una incapacità di intendere e di volere. Ciò avrebbe comportato “*l'impossibilità di fare altrimenti e quindi di autodeterminarsi*” e, in ultima istanza, il vizio totale di mente¹⁴⁴.

Sono opposte, invece, le conclusioni cui perviene la perizia disposta dal giudice, in quanto in essa – pur riconoscendosi l'incidenza del tumore sulla regione orbito-

¹⁴¹ *Ibidem*.

¹⁴² Greenwald, A., G., McGhee, D., E., Schwartz, J., K., L., *Measuring individual Differences in Implicit Cognition: The Implicit Association Test*, in *Journal of Personality and Social Psychology*, 74, 1998, pp. 1464-1680.

¹⁴³ Tribunale di Venezia, G.i.p. dott.ssa Marchiori, 24 gennaio-8 aprile 2013, sent. n. 296, p. 16.

¹⁴⁴ Estratto della perizia riportata nella sentenza, p. 17.

frontale, viene censurata la connessione causale tra la massa tumorale e l'orientamento sessuale. Inoltre, il ricorso allo a-IAT, oltre a difettare del carattere della utilizzabilità sotto il profilo processuale, è incorso nella censura di difetto del preponderante consenso della comunità scientifica, essendo ancora in fase di sperimentazione¹⁴⁵.¹⁴⁶ Questa sentenza consente di osservare i contrapposti approcci teorici in azione. In particolare, quello a cui si assiste è un vero e proprio contraddittorio sulla prova scientifica, il quale permette una valutazione delle prove più mature da parte del giudice. Innanzitutto, l'estensore esclude la possibilità di aderire alla tesi della correlazione tra “alcune patologie di carattere organico e l'orientamento pedofilo”¹⁴⁷, in quanto tale ipotesi “trova oggi riscontro in un numero assai limitato di casi”¹⁴⁸; il Tribunale dimostra, dunque, di aver valutato criticamente la teoria prospettata, verificandone la diffusione nel campo scientifico.

¹⁴⁵ Ai sensi dell'art. 188 c.p.p., infatti: “*non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti*”. Diversamente è stato valutato dal giudice di Cremona nella sent. 823/2012 il quale ha affermato che “*tali metodologie nulla hanno a che vedere con gli antiquati tentativi di verificare la sincerità di un soggetto tramite lie detectors o poligrafi, strumenti che pretenderebbero di fondare la valutazione su grossolani sintomi psico-fisici del periziando*”. La tecnica, quindi, andrebbe valutata secondo il parametro Daubert valutando “*precedenti verifiche e cioè falsificabilità della teoria in senso popperiano e quindi resistenza del metodo a tentativi di smentita, controllo dei lavori pubblicati da parte di revisori qualificati (peer review), accettabilità dei limiti di errore, accoglimento da parte della comunità scientifica*”. Cfr. Cassazione penale, Sez. IV, 13 dicembre 2010 (17 settembre 2010), n. 43786 - Pres. Marzano - Est. Blaiotta - P.M. Delehay (diff.) - Cozzini e altri.

¹⁴⁶ Farano, A., *La responsabilità giuridica alla prova delle neuroscienze*, Bari, Cacucci Editore, 2018, pp. 160-161.

¹⁴⁷ Trib. Venezia, G.i.p., 24 gennaio 2013, n. 296, imp. Mattiello, In *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2013, n. 4. p. 1907.

¹⁴⁸ *Ibidem*.

2.4 Emozioni, informatica ed ingegneria sociale

Il giurista italiano che maggiormente si è dedicato alle nuove ricerche cognitive sulla mente dell'uomo e sulla modellizzazione del ragionamento giuridico in schemi logici suscettibili di applicazione informatica è Giovanni Sartor il quale, dalle scienze cognitive, trae la concezione della mente umana come un insieme di competenze diverse che conducono l'agente al volere e alla realizzazione dell'atto desiderato. Inoltre, osserva che, se si vuole comprendere e prevedere il comportamento delle persone, è necessario presupporre che esse posseggano stati cognitivi, cioè che passino da uno stato cognitivo ad un altro. Soltanto così sarà possibile prevedere il comportamento di soggetti diversi¹⁴⁹.

Tuttavia, la mente umana non è infallibile, come spesso pensiamo, anzi, sono infiniti i fenomeni di mispercezione che hanno luogo quando i dati sensoriali arrivano al cervello in modo non corretto, facendoci avvertire una realtà diversa da quella che è concretamente. La mente, quindi, ci inganna di continuo e questa mistificazione ha un'origine strettamente connessa all'universo delle emozioni, poiché esse forniscono la risposta automatica agli stimoli, che ci proteggono e ci permettono di riconoscere i pericoli. Quando, però, la loro intensità diventa eccessiva o quando non riusciamo a controllarle, corriamo il rischio che queste ci si rivoltino contro. È in tali casi che entra in gioco l'ingegneria sociale, connubio di sicurezza informatica e neuroscienze, una vera e propria arte che sfrutta la psicologia, le vulnerabilità umane e la comunicazione per ingannare la vittima.

Gli attacchi di *social engineering*, infatti, puntano proprio alla sfera emotiva per portare le vittime a compiere azioni immediate, conseguenze di emozioni non controllabili.

Con ciò, si dimostra la stretta relazione che si viene a creare tra conoscenza informatica, antropologia, psicologia e neuroscienze.

¹⁴⁹ Romeo, F., *Lezioni di logica ed informatica giuridica*, Torino, Giappichelli, 2012, pp. 161-167.

Quello che rende, di fatto, questi attacchi tanto dannosi è che non presentano alcuna componente tecnica specifica, ma sfruttano esclusivamente leve psicologiche come le emozioni e l'istinto, elemento centrale del cervello rettiliano¹⁵⁰.

Quando le persone si trovano di fronte a qualcosa di spaventoso, come una minaccia, la valutano naturalmente e considerano quanto sia reale per applicare i comportamenti raccomandanti al fine di evitarla.

Per poter, quindi, contrastare gli attacchi di ingegneria sociale è necessario adottare un approccio multidisciplinare che affianchi alle competenze tecnologiche, quelle umanistiche e relazionali. Per cui, da un lato serve investire in tecnologie avanzate capaci di identificare i cambiamenti messi in atto dall'industria del *cybercrime*¹⁵¹; dall'altro serve intervenire sull'essere umano affinché la consapevolezza delle proprie emozioni possa aiutarlo ad essere meno impulsivo e a reagire in modo più razionale agli stimoli.

Guardando all'economia comportamentale, alla psicologia, alla sociologia, alle neuroscienze e ad altri campi è possibile comprendere i pregiudizi cognitivi per coinvolgere meglio le persone a migliorare la consapevolezza, il comportamento e la cultura della *cybersicurezza*, di cui ci occuperemo nel capitolo successivo di questo elaborato. Quando si tratta di aumentare la consapevolezza sulla sicurezza informatica, risultano particolarmente rilevanti cinque euristiche (scorciatoie nel cervello) che hanno una notevole influenza su come le persone si comportano; queste sono la prova

¹⁵⁰ Il cervello rettiliano, teorizzato dal neurologo americano Paul MacLean, consiste nella più antica struttura anatomica del cervello umano. Questa parte del cervello corrisponde al tronco cerebrale e al cervelletto ed è equiparabile al cervello di un rettile, affidabile ma rigido e compulsivo. Il cervello rettiliano è considerato uno dei tre livelli di evoluzione del cervello umano, il più primitivo, che ha accesso solo alla memoria a breve termine e quindi agisce secondo automatismi. Cfr. MacLean, P., D., *The Triune Brain in Evolution: Role in Paleocerebral Functions*, Springer, 1990.

¹⁵¹ V. par. 3.2 cap. III.

sociale, il bias dell'ottimismo, la psicologia della paura, la minaccia degli stereotipi e l'autoefficacia.

La prova sociale risulta familiare alla maggioranza degli individui poiché la sua influenza sul comportamento è stata esplorata in molte discipline. Per farne un esempio, il fatto che un consumatore noti che un servizio è ben recensito aumenta la probabilità che anch'egli voglia provarlo.

Il *bias* dell'ottimismo porta le persone a sottovalutare la probabilità che accadano cose brutte nel loro futuro e sopravvalutano quella che accadano cose belle.

Negli ultimi dieci anni, una ricerca condotta da un team di neuroscienziati ha scoperto che circa l'80% delle persone è predisposta ad essere ottimista,¹⁵² a nulla rilevando la tipologia di messaggi o fatti che viene trasmessa alle persone: queste rimarranno ottimiste. Così a titolo di esempio, nell'area della sicurezza informatica non ha rilevanza mettere al corrente le persone circa la probabilità che vengano violati gli *hacking* e l'influenza dannosa che da ciò possa conseguire, perché le persone manterranno il loro ottimismo. Quando i professionisti della sicurezza informatica si trovano di fronte ad una persona non qualificata che mostra questo tipo di ostinato ottimismo, di solito rispondono con più fatti, fornendo statistiche circa la quantità di attacchi che si verificano, o la quantità di denaro che verrà sbordato dall'utente. Nonostante ciò, le persone difficilmente cambiano idea, tuttavia l'ottimismo fa sì che si impegnino di più e siano più propense a cambiare nei comportamenti che vengono raccomandati per ridurre le minacce.

La terza euristica, la psicologia della paura deve essere gestita molto attentamente per stimolare un cambiamento positivo del comportamento. L'approccio tradizionale della sicurezza informatica è stato profondamente radicato nella paura, nell'incertezza e nel dubbio. Dire alle persone cose spaventose, con l'intento di migliorare il

¹⁵² Sharot, T., *The Optimism Bias: Why We're Wired to Look on the Bright Side*, London, Robinson, 2012.

comportamento, non funziona. In materia è stata condotta una ricerca nota come “*fear appeals*”: usare la paura per cercare di cambiare il comportamento¹⁵³. Ciò che è stato dimostrato è che per usare un messaggio spaventoso in modo efficace, è necessario comunicarlo con molta attenzione. Quando una persona si trova davanti ad una minaccia tende a valutarla e a considerare quanto possa essere reale. Soltanto quando si renderà conto della serietà della stessa, applicherà i comportamenti raccomandati per evitarla. Gli appelli alla paura possono, quindi, essere un modo molto dannoso per diffondere il messaggio sulla sicurezza informatica. Un modo molto più efficace di comunicare la sicurezza informatica è quello di evidenziare gli aspetti positivi che derivano da un buon utilizzo della stessa.

Ulteriore euristica è la minaccia dello stereotipo. Il suo peso fa sì che le persone lo confermino involontariamente. Se individui o gruppi entrano in una situazione in cui sanno di essere oggetto di uno stereotipo, la loro consapevolezza costituirà un peso e una distrazione tale che finiranno per conformarsi ad esso. Su questo tema sono state condotte interessanti ricerche. Se siamo in presenza di uno stereotipo, questo può essere così dannoso per gli individui che non otterranno le stesse prestazioni che normalmente avrebbero reso. Quando si parla di sicurezza informatica, uno stereotipo che domina con forza questo settore è la percezione che le persone sono l'anello debole del sistema, al punto da rappresentarne il problema.

L'ultima scorciatoia del cervello che influenza il comportamento umano è l'autoefficacia, che consiste nella maggiore convinzione di una persona di poter avere successo in situazioni specifiche o di portare a termine un compito, determinando comportamenti migliori. Questo si evince dalle ricerche condotte non solo sui livelli

¹⁵³Witte, K., Allen, M., *A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns*, *Health Education & Behavior: The Official Publication of the Society for Public Health Education* 27, 2000; Ruiter, R., Loes, T., E., Kessels, G. Y., Peters, G., K., *Sixty Years of Fear Appeal Research: Current State of the Evidence*, *International Journal of Psychology* 49, n. 2, 2014.

di *empowerment* e di autoefficacia, ma anche sui livelli di fiducia nella sicurezza informatica¹⁵⁴. Queste ricerche hanno rilevato che le persone che si sentono più sicure della sicurezza informatica sono più propense a mettere in atto i comportamenti che vengono raccomandati, come ad esempio effettuare gli aggiornamenti, avere un approccio forte alle *password*, utilizzare una buona “igiene informatica”. Se alle persone vengono forniti l’incoraggiamento e gli strumenti necessari, queste metteranno in pratica comportamenti più sicuri. Quando si parla di sicurezza informatica, ci si riferisce inevitabilmente a circostanze che fanno paura: minacce, crimini e comportamenti dannosi. Le persone possono spesso sentirsi intimidite dall’argomento, per questo i messaggi di efficacia sono così importanti. Se i professionisti della sicurezza informatica parlano di qualcosa di spaventoso senza fornire un forte messaggio di efficacia, gli ascoltatori si impegneranno a controllare la risposta emotiva alla paura piuttosto che a controllare il pericolo stesso.

“Se gli appelli alla paura vengono diffusi senza messaggi di efficacia, o con una raccomandazione di una sola riga, corrono il rischio di ritorcersi contro, in quanto possono produrre risposte difensive in persone con percezioni di bassa efficacia”¹⁵⁵.

La ricerca psicologica ha dimostrato l’importanza di responsabilizzare le persone e di aumentare il loro senso di autoefficacia per modificare positivamente i loro comportamenti.

Queste cinque scorciatoie del cervello si riferiscono al modo in cui inquadrano i nostri messaggi. Con una comprensione più approfondita della psicologia, dell’economia comportamentale, delle neuroscienze e della sociologia, possiamo

¹⁵⁴ Rhee, H., Cheongtag, K., Ryu, Y., *Self-Efficacy in Information Security: Its Influence on End Users’ Information Security Practice Behavior*, Computers & Security 28, n. 8, 2009.

¹⁵⁵ Witte, K., Allen, M., *A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns*, Health education & behavior: the official publication of the Society for Public Health Education, 2020, pp. 606-607.

renderli molto più coinvolgenti e di maggiore impatto. Sfruttando a nostro favore la prova sociale e l'ottimismo, diffondendo la speranza invece della paura, resistendo agli stereotipi e aumentando l'autoefficacia, possiamo essere più efficienti nella nostra sensibilizzazione sulla sicurezza informatica, arrivando così ad un cambiamento comportamentale più positivo e a culture della sicurezza informatica più forti¹⁵⁶.

A conclusione del capitolo, è possibile dare per assodato che sia utile sapere come funzioniamo, cosa succede al nostro cervello e al nostro corpo così da poter riconoscere le emozioni e assegnarle un significato, tutto ciò con notevoli benefici nel campo del cd. *human hacking*.

¹⁵⁶ Barker, J., *The human nature of cybersecurity*, Educause Review 54, n. 2, 2019, <https://er.educause.edu/-/media/files/articles/2019/5/er192104.pdf> , data ultima visualizzazione 20/01/2023.

CAPITOLO III

CYBERSECURITY E RESPONSABILITÀ IN RETE

SOMMARIO: 3.1 Introduzione alla *cybersecurity*: nascita e sviluppo del *cyberspace*. – 3.1.1 Tipologie di *cyberattacks*. – 3.1.1.1 *Malware*. – 3.1.1.2 *Ransomware*. – 3.1.1.3 *Phishing*. – 3.1.1.4 *Pharming*. – 3.2 Dalla *cybersecurity* al *cybercrime*: criminalità informatica. – 3.2.1 Reati informatici nel diritto. – 3.3 *Cyberattacchi* e COVID-19: virus a confronto. 3.3.1 Danni subiti dalle aziende: strategie e modelli organizzativi per le imprese.

3.1 Introduzione alla *cybersecurity*: nascita e sviluppo del *cyberspace*

L'evoluzione tecnologica e informatica dello scorso secolo ha contribuito alla trasposizione del fulcro delle attività sociali, politiche ed economiche, giungendo alla nascita di una nuova dimensione, quella del *cyberspace*. Questo “spazio cibernetico” dipinge un nuovo dominio, trasversale ai quattro tradizionali (terrestre, aereo, marittimo, spaziale), nel quale l'avanzare delle nuove tecnologie e dell'intelligenza artificiale avranno un ruolo determinante, al pari di quello degli esseri umani.

Il termine *cyberspace* risale a William Gibson, scrittore statunitense del '900, il quale nel 1982 ne ha fatto uso in *Burning Chrome*, un racconto di fantascienza e successivamente nel romanzo *Neuromancer*. Gibson utilizza questo termine per fare riferimento ad un luogo immaginario di allucinazioni tecnologiche composto da dati, in cui uomini e computer si fondono per creare un'unica realtà, contrapposta allo spazio reale¹⁵⁷.

Il *cyberspazio*, negli anni e con l'avvento di Internet, sta subendo una serie di ampliamenti a ritmi accelerati, spostando sempre più in avanti il limite di ciò che in

¹⁵⁷ Cfr. Gibson, W., *Neuromance*, 1986.

esso può essere eseguito¹⁵⁸, oltre a far assumere all'espressione *cyberspace* un significato differente. A partire, infatti, dalla prima metà degli anni Novanta del secolo scorso, indica un ambiente informatico volto allo scambio di informazioni attraverso sistemi interconnessi¹⁵⁹. Presenta tre caratteristiche: giovinezza, modernità e autorganizzazione. È giovane perché solo nel 1991 nasce il *World Wide Web*, uno dei più importanti servizi di Internet. È moderno perché in grado di adeguarsi a qualsiasi cambiamento in un mondo in continua evoluzione. Inoltre, è autorganizzato in quanto capace di rispondere "autonomamente" alle modificazioni cui è soggetto¹⁶⁰.

Il *Cyberspace*, lo spazio cibernetico¹⁶¹, non coincide con il sistema di reti di telecomunicazioni e, quindi, con Internet, ma si tratta di uno spazio virtuale più ampio.

¹⁵⁸ Cfr. Scardovi, G., *Mondo che genera mondo: memoria, codice, cyberspazio*, in "Politica & Società, Periodico di filosofia politica e studi sociali" 1/2018, p. 5: "[...] si è preso a considerarlo come l'esito di un non controllabile processo di proliferazione autoindotta di flussi di informazione onnipervasivi, dotati di una forza di penetrazione priva di equivalenti in ogni altro campo dell'intervento tecnico umano. Richiamandosi ai differenti motivi della rapida espansione e della pervasività, lo si è quindi descritto sia come una sorta di immenso blob, inglobante via via tutto ciò che incontra sulla sua strada, senza esitazioni, sia ricorrendo alla spaventosa idea di un Grande Fratello che spia chiunque, in ogni momento".

¹⁵⁹ Martino, L., *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, Fascicolo 1/2018, pp. 61 ss.

¹⁶⁰ Harries, D., *Narrative Mapping of Cyberspace. Context and Consequences*, in Ramírez Luis, J., M., García-Segura, A., (Cur.), *Cyberspace Risks and Benefits for Society, Security and Development*, Berlino, Springer, 2017, pp. 23-40.

¹⁶¹ "Disciplina che si occupa dello studio unitario dei processi riguardanti «la comunicazione e il controllo nell'animale e nella macchina» (secondo la definizione di N. Wiener, 1947): partendo dalle ipotesi che vi sia una sostanziale analogia tra i 'meccanismi di regolazione' delle macchine e quelli degli esseri viventi e che alla base di questi meccanismi vi siano processi comunicazione e di analisi di informazioni, la cybersecurity si propone da un lato di studiare e di realizzare macchine ad alto grado di automatismo, atte a sostituire l'uomo nella sua funzione di controllore e di pilota di macchine e di

Ad oggi non esiste un'unica definizione per questo termine¹⁶², tuttavia il *cyberspazio* può essere definito quale insieme di infrastrutture informatiche tra loro connesse, costituito da *hardware*, *software*, dati ed utenti e relative relazioni intercorrenti tra essi¹⁶³.

Una “peculiarità” è che alla sua formazione concorrono sia elementi naturali che virtuali e questa natura “ibrida” porta a considerare complessa la possibilità di una condivisione onnicomprensiva della descrizione cognitiva del termine *cyberspace*^{164, 165} che in sintesi, comprende Internet e le reti di comunicazione, nonché i sistemi informatici in cui vengono elaborati i dati, caratterizzandosi per la sua connotazione dematerializzata, deterritorializzata, atemporale e inoltre, caratteristica ad esso peculiare, per la garanzia dell'anonimato.

impianti, e dall'altro lato, inversamente, di servirsi delle macchine anzidette per studiare determinate funzioni fisiologiche e dell'intelligenza”. Voce “cibernetica”, in *Enc. Online Treccani*, www.treccani.it.

¹⁶² Secondo F. D. Kramer esistono 28 definizioni diverse del termine *cyberspace*. Cfr. Kramer, Starr, Wentz 2009. L'etimologia della parola “*cyber*” o “cibernetica” può essere ricollegata al termine greco κυβερνήτης, che significa “dirigere” o “navigare”. Tuttavia, volendo ricercare una radice etimologica della parola “*cyberspace*” possiamo riprendere la prima definizione storica coniata da William Gibson nel 1984 che descrive il *cyberspace* come “*A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concept. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding*”, cfr. Gibson, W., *Neuromancer*, 1984.

¹⁶³ V. Mensi, M., *La sicurezza cibernetica*, in Mensi, M., Falletta, P., *Il diritto del web*, Cedam, 2018, p. 281.

¹⁶⁴ Cfr. Nye 2011. Tuttavia, persiste una diatriba più generale anche in merito a tutte le definizioni che includono il prefisso “*cyber*”: *cyber-terrorism*, *cyber-war*, *cyber-weapons*, *cyber-operations*, ecc...

¹⁶⁵ Martino, L., *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica & Società, Periodico di filosofia politica e studi sociali" 1/2018, pp. 61-76.

Questi requisiti contraddistinguono le condotte che si esplicano in rete rispetto a quelle che avvengono al di fuori di essa, dal momento in cui un soggetto può svolgere un'operazione complessa, collegandosi, anche contemporaneamente, a più siti virtuali. Tutto ciò rende problematica l'applicazione di quei principi che necessitano l'individuazione del luogo in cui viene realizzata l'azione. È perciò evidente che è un compito arduo cercare di rappresentare un ambiente virtuale tramite le dinamiche e i concetti degli spazi reali¹⁶⁶. La *National Military Strategy for Cyberspace Operations* (NMS-CO) del 2006 descrive il *cyberspazio* tramite l'acronimo *VUCA: Volatility, Uncertainty, Complexity, Ambiguity*¹⁶⁷. La velocità di propagazione e l'assenza di confini caratterizzano l'ambiente cibernetico, in cui tutto si evolve in base alle scoperte tecnologiche e scientifiche¹⁶⁸.

Nonostante esso sia privo di confini territoriali, è dunque compito della *cybersecurity* assicurarne la sicurezza, proteggendo reti ed infrastrutture, aziende e singoli.

In quanto artificiale, il dominio cibernetico presenta infatti molte "vulnerabilità", punti di debolezza tramite i quali è possibile acquistare illegalmente dati e informazioni che passano attraverso di esso, oppure compromettere il funzionamento di servizi e sistemi digitali¹⁶⁹.

L'obiettivo degli Stati è quello di arginare le minacce che provengono dalla dimensione cibernetica, solitamente rivolte ad infrastrutture fisiche, alle attività produttive e ai loro stessi sistemi di sicurezza. Queste condotte minacciose risultano difficili da perseguire per la caratteristica tipica del *cyberspazio* quale luogo garantito

¹⁶⁶ Cfr. Gray 2013.

¹⁶⁷ Cfr. Sherrer e Grund 2009.

¹⁶⁸ Martino, L., *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica & Società, Periodico di filosofia politica e studi sociali" 1/2018, p. 66.

¹⁶⁹ Aterno, S., *Sicurezza informatica: aspetti giuridici e tecnici*, Pacini Giuridica, Pisa, 2022, p. 209.

da anonimato, oltre al fatto che possono essere commesse da grandi distanze, essendo sufficiente un accesso alla rete.

Spesso queste minacce sfruttano le vulnerabilità tecniche e organizzative dovute ad una lacuna nella sicurezza. È, quindi, compito degli Stati e principale sfida per la moderna società dell'informazione garantire la sicurezza per prevenire ed evitare questi fenomeni ad oggi in costante crescita¹⁷⁰.¹⁷¹

Al riguardo, il Consiglio dei ministri, nella seduta del 19 settembre 2019, ha approvato il decreto-legge del 2019, n. 105 (pubblicato in Gazzetta Ufficiale il 21 settembre 2019) che introduce disposizioni urgenti in materia di “perimetro” di sicurezza nazionale cibernetica¹⁷². Il D.L. mira ad assicurarne un elevato livello nell'ambito dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, tramite l'istituzione di un perimetro che ne garantisca i necessari standard rivolti a minimizzare i rischi consentendo, nel mentre, l'utilizzo dei più avanzati strumenti offerti dalle tecnologie dell'informazione¹⁷³.

La minaccia cibernetica non è da sottovalutare, anzi, viene considerata come pericolo rilevante, in rapida evoluzione, capace di produrre effetti a distanze non raggiungibili con gli ordinari strumenti di attacco. Infatti, i *cyberattacchi* possono avere origine da qualsiasi luogo riuscendo a compromettere l'integrità della rete informatica di un paese intero. Inoltre, le attività preventive e di contrasto sono difficili da porre in essere in

¹⁷⁰ Il Rapporto Clusit 2021 sulla sicurezza ICT in Italia ha previsto un aumento degli attacchi con finalità di “*Cybercrime*” del 10% rispetto all'anno precedente, https://www.mmn.it/wp-content/uploads/2022/03/Rapporto-Clusit-marzo-2022_c_web.pdf, data ultima visualizzazione 29/01/2023.

¹⁷¹ V. par. 3.2.

¹⁷² Decreto-legge 21 settembre 2019, n. 105 recante: “*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*”.

¹⁷³ Aterno, S., *Sicurezza informatica: aspetti giuridici e tecnici*, Pacini Giuridica, Pisa, 2022, p. 210.

quanto risulta complesso tracciare gli attacchi medesimi. Sono, infatti molteplici le figure che si muovono nel *cyberspace* con finalità diverse e difficilmente identificabili che vanno dall'*hacker* individuale che agisce a scopo di lucro, all'organizzazione criminale, fino all'apparato governativo. Si spazia, quindi, dal vandalismo cibernetico alla vera e propria guerra cibernetica.

La velocità degli attacchi e la difficoltà a prevenirli hanno reso particolarmente vulnerabili anche i paesi maggiormente evoluti sul piano militare, i quali avvertono la necessità di definire adeguate misure di difesa rispetto ad agenti di natura volontaria o non che potrebbero alterare dati e servizi fondamentali del paese.

3.1.1 Tipologie di *cyberattacks*

L'espansione della digitalizzazione ha aumentato l'utilizzo di dispositivi informatici e l'accesso alla rete per un numero sempre maggiore di utenti. Ciò ha creato nuove vulnerabilità nei sistemi e nei dati informatici esponendo un numero crescente di potenziali vittime e attori delle minacce. Per un certo verso ha portato molti vantaggi, come una maggiore efficienza nella gestione delle risorse e nella comunicazione, ma ha anche aumentato i rischi per la sicurezza informatica. Con un numero sempre maggiore di utenti che utilizzano dispositivi informatici e accedono alla rete, ci sono più opportunità per gli aggressori di attaccare i sistemi e rubare dati sensibili. Infatti, il rapido evolversi della tecnologia sta rendendo difficile l'esistenza di sistemi completamente sicuri.

Il *cyberattacco*, definito come il tentativo di ottenere un accesso non autorizzato a servizi, risorse al fine di comprometterne l'integrità, in generale consiste nell'atto intenzionale di eludere uno o più servizi di sicurezza o controlli di un sistema¹⁷⁴.

¹⁷⁴ “National Initiative for Cybersecurity Careers and Studies”, www.niccs.us-cert.gov, data ultima visualizzazione 29/01/2023.

Il Regolamento sulla *cybersicurezza* definisce la minaccia informatica come “qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone”¹⁷⁵.

A seconda degli obiettivi, le minacce informatiche possono essere suddivise in cinque macro-categorie: l'*hacktivismo*, che ha principalmente scopi dimostrativi e cerca di danneggiare la reputazione; il *cybercrime*, che colpisce soprattutto il settore privato e si rivolge ad attività con finalità criminali, per ottenere denaro o rubare informazioni per trarne profitto; il *cyberspionaggio*, che prende di mira informazioni industriali e scientifiche; il *cyberterrorismo*, con azioni ideologicamente motivate e indirizzate a Stati e individui; la guerra cibernetica, che consiste in operazioni militari effettuate nel *cyberspace*.

Inoltre, gli attacchi informatici si distinguono in attacchi cosiddetti semplici o complessi, a seconda che siano posti in essere rispettivamente tramite un'unica operazione ovvero tramite più operazioni tra loro collegate. Possono essere indirizzati sia a infrastrutture fisiche, *hardware* e server, sia a soluzioni *software* essenziali per il funzionamento dei sistemi e della rete.

Altro elemento che caratterizza le tipologie di attacchi informatici è l'utilizzo o meno della violenza: questi, infatti, possono essere commessi danneggiando i sistemi informatici, oppure realizzati mediante condotte fraudolente in cui vi è la cooperazione artificiosa della vittima¹⁷⁶.

¹⁷⁵ Art. 2 n. 8, Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, *Cybersecurity Act*.

¹⁷⁶ Cfr. Flor, R., *Cybersecurity ed il contrasto ai cyber-attacks*, in DIRITTO DI INTERNET, n. 3, 2019, p. 454.

3.1.1.1 *Malware*

Il *malware* è un *software* malevolo progettato per danneggiare, rubare o compromettere i sistemi informatici al fine di estorcerne i dati personali e rappresenta la più comune tipologia di attacco in grado di colpire sistemi, dispositivi e reti senza il consenso dell'utente mediante l'interferenza con le classiche operazioni svolte da un computer.

Il *malware* agisce innanzitutto introducendosi nel sistema, tramite una serie di canali quali ad esempio la posta elettronica¹⁷⁷ o i siti *web*, riuscendo ad eludere le eventuali misure di protezione predisposte e ingannando l'utente vittima che inconsapevolmente "fornisce aiuto"¹⁷⁸.

Una volta che il *software* viene inserito nel sistema resta silente fino al momento della sua attivazione e, quindi, al momento in cui vengono eseguiti gli obiettivi dell'attacco. Esistono varie tipologie di *malware*: i *virus* sono i più comuni, progettati per replicarsi all'interno dei sistemi informatici, danneggiando o cancellando i dati. Essi si diffondono attraverso allegati *e-mail*, *file* condivisi e *download* di *software* dannoso¹⁷⁹. Un'altra tipologia di *malware* è rappresentata dal *worm*¹⁸⁰, simile al *virus*, ma a differenza di questo, si diffonde autonomamente attraverso una rete, utilizzando le vulnerabilità dei sistemi per infettare altri computer.

¹⁷⁷ In questo caso, mediante tecniche di ingegneria sociale, l'utente vittima apre gli allegati di posta elettronica infetti, fornendo così un consenso involontario.

¹⁷⁸ Cfr. Mezzalama, M., Liroy, A., Metwalley, H., *Anatomia del malware*, in Riv. Mondo Digitale, 47/2013, pp. 3 ss.

¹⁷⁹ Cuomo, L., Razzante, R., *La nuova disciplina dei reati informatici*, Torino, Giappichelli, 2007, p. 122.

¹⁸⁰ L'attacco "*I love you*" è considerato uno degli attacchi *worm* più famosi. Scoperto nel 2000, questo attacco è riuscito a colpire milioni di computer mediante l'invio di una *mail* contenente un allegato contenente il testo "*I love you*". Una volta che l'utente apriva l'allegato, il *worm* iniziava ad autoriprodursi

Esiste, inoltre, il *trojan horse*, un programma dannoso nascosto nel *software* e apparentemente innocuo. Una volta installato, può aprire le porte del sistema per l'accesso remoto da parte di *hacker*. Questa tipologia di attacco ha la capacità di auto propagarsi, quindi, deve essere inviato alla singola macchina che il soggetto agente ha intenzione di infettare.

In caso di infezione da *malware*, è importante eseguire la scansione del sistema con un *software* *antivirus* e seguire le istruzioni per rimuoverlo. In alcuni casi, potrebbe essere necessario anche ripristinare il sistema riportandolo a un punto precedente all'infezione.

È fondamentale prevenire il *malware* mediante l'utilizzo di *software* *antivirus* e *firewall*, nonché con l'adozione di buone pratiche di sicurezza come l'evitare di aprire *mail* di mittenti sconosciuti o di scaricare *software* da fonti non attendibili.

3.1.1.2 Ransomware

Il *ransomware* è una tipologia di *malware* estorsivo, che crittografa i dati dell'utente e li rende inaccessibili fino a quando non viene pagato un riscatto, spesso sotto forma di criptovalute. Ad oggi rappresenta la tipologia di *malware* più diffusa¹⁸¹.

inviando copie ai contatti in rubrica con il nome dell'utente come mittente. Questo causava il rallentamento del computer e successivamente l'inutilizzo. Si stima che questo attacco abbia causato danni per 10 miliardi di dollari. Cfr. Lana, A., *I love You, venti anni fa il primo virus informatico che ha messo il mondo in ginocchio*, in www.corriere.it, 4 maggio 2020, data ultima visualizzazione 29/01/2023.

¹⁸¹ Secondo il rapporto CLUSIT 2020, nel 2019 i *ransomware* sono stati quasi la metà del totale degli attacchi di tipo *malware*. Cfr. Analisi delle principali categorie di *malware*, in Rapporto CLUSIT 2020, 2020, 29, in www.clusit.it, data ultima visualizzazione 30/01/2023.

Ciò che lo caratterizza è la sua condotta bifasica: in un primo momento avviene un attacco mediante l'introduzione e la compromissione del sistema; successivamente viene posta in essere la fase della minaccia seguita dalla richiesta di riscatto. Una volta che la vittima effettua il pagamento, riceverà le indicazioni per effettuare la decriptazione, anche se spesso il *malware* cancella definitivamente i dati o rende inservibile il sistema.

Il *ransomware* è una minaccia in continua crescita che può causare danni significativi sia alle aziende che agli individui. Una volta che il sistema viene infettato, l'*hacker* può anche utilizzare il *malware* per rubare informazioni sensibili o utilizzare il computer infetto come punto di ingresso per ulteriori attacchi.

Per evitare di essere vittima di un attacco *ransomware* è importante seguire alcune pratiche di buona sicurezza, come mantenere i *software* aggiornati, utilizzare un *software* antivirus affidabile, eseguire *backup* regolari dei dati. Inoltre, è fondamentale non aprire allegati o collegamenti sospetti in *e-mail* o messaggi di testo, poiché questo riesce ad accedere ai sistemi grazie alla vulnerabilità degli utenti.

L'attacco *ransomware* "*WannaCry*" è stato uno dei più grandi della storia (oltre 200.000 sistemi informatici colpiti in tutto il mondo nel 2017), mediante il quale il *malware* si è diffuso attraverso un *exploit* chiamato *EternalBlue*, sviluppato dall'agenzia di sicurezza nazionale degli Stati Uniti, che ha sfruttato una vulnerabilità del protocollo di condivisione di *file* di rete *SMB* (*Server Message Block*) su computer con sistema operativo *Windows* non aggiornato.

Una volta che un computer è stato infettato, *WannaCry* si è propagato a tutti gli altri sistemi sulla rete che usufruiscono delle condivisioni *SMB*. Il *malware* ha criptato i *file* e ha chiesto un riscatto in *bitcoin* per decifrarli, anche se, pagare il riscatto non garantiva il ripristino dei dati.

Gli obiettivi principali di *WannaCry* sono stati gli ospedali e gli enti pubblici, che spesso hanno sistemi meno aggiornati rispetto alle grandi aziende. *Microsoft* aveva rilasciato un aggiornamento gratuito per proteggere i sistemi dall'*exploit* *EternalBlue*,

ma molti utenti non l'hanno installato in tempo. L'attacco di *WannaCry* ha causato perdite per diversi miliardi di dollari e ha dimostrato l'importanza di mantenere i sistemi informatici aggiornati e di avere una buona cultura della sicurezza informatica. Inoltre, è stato un ulteriore promemoria sull'importanza di fare *backup* regolari dei dati per poterli ripristinare in caso di attacco¹⁸².

3.1.1.3 *Phishing*

Il *phishing* è una forma di frode informatica¹⁸³ che mira a ottenere informazioni personali sensibili, come *password* o numeri di carte di credito, attraverso l'inganno ed è nato come tecnica di *social engineering*, tramite condotte che riescono ad ingannare la vittima con lo scopo di carpire determinate informazioni.

¹⁸² V. Dal Checco, P., Il ransomware Wannacry infetta PC non aggiornati: ospedali ed enti pubblici a rischio, 12 maggio 2017, in www.ransomware.it, data ultima visualizzazione 30/01/2023.

¹⁸³ “*Chiunque, alterando in qualsiasi modo il funzionamento di sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da trecentonove euro a millecinquecentoquarantanove euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.*

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età”, art. 640-ter c.p.

Il termine *phishing* deriva probabilmente dall'unione dei termini inglesi “*phreaking*” e “*fishing*” – il primo facente riferimento all'uso di frequenze per manipolare un sistema telefonico, mentre il secondo la cui traduzione letterale è “pescare”, allude alla pesca dei dati dell'utente tramite il *web*¹⁸⁴.

I truffatori, solitamente, mediante l'invio di *e-mail* ingannevoli o l'utilizzo di siti *web* falsi chiedono alla vittima di fornire informazioni personali o di fare clic su un *link* che porta a un sito *web* compromesso. Generalmente l'obiettivo del *phisher* è quello di indurre l'utente a rivelare le credenziali e i codici per accedere ai servizi bancari *online* per poi rubare l'identità delle vittime.

I messaggi, il più delle volte, vengono formulati *ad hoc* e contengono notizie che possono sembrare reali, come ad esempio la necessità di dover aggiornare i propri dati bancari cliccando su un determinato *link*. Così facendo l'utente “abbocca all'amo” e viene ingannato.

Il *phishing* è diventato sempre più sofisticato negli ultimi anni e la crescita continua del numero di attacchi non consente una disciplina giuridica *ad hoc* che consideri unitariamente il fenomeno in questione.

Per difendersi dal *phishing* è fondamentale rimanere diffidenti nei confronti di *e-mail* o siti *web* che chiedono informazioni personali. Inoltre, è importante utilizzare un *software* di sicurezza aggiornato per proteggere il proprio dispositivo da eventuali attacchi informatici.

¹⁸⁴ Flor, R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in Riv. it. dir. proc. pen., 2007, pp. 903 ss.

3.1.1.4 *Pharming*

Il *pharming* rientra tra gli attacchi complessi in quanto l'*iter criminis* consta di svariate azioni, commesse in tempi diversi.

Esso mira ad ottenere informazioni personali sensibili, come le credenziali di accesso a un conto bancario o a una carta di credito, attraverso la manipolazione dei siti *web* legittimi. È spesso combinato con il *phishing*, in quanto entrambi condividono l'obiettivo finale, cioè acquisire abusivamente dati sensibili. Tuttavia, il *pharming* è più subdolo del *phishing* perché gli utenti possono essere indotti a inserire informazioni personali su un sito *web* che sembra legittimo, ma che in realtà è stato manipolato per rubarle. La manipolazione può essere effettuata tramite una serie di tecniche, come l'utilizzo di un *software* dannoso o l'alterazione del sistema *DNS* (*Domain Name System*).

Può essere particolarmente pericoloso perché le vittime vengono incitate a fornire informazioni personali, senza rendersi conto di essere ingannate. Inoltre, gli utenti possono essere indotti a cliccare su un *link* che li reindirizza a un sito *web* non autentico, dove possono essere invitati a inserire informazioni personali.

Per proteggersi dal *pharming*, gli utenti devono essere consapevoli dei rischi e adottare precauzioni, come l'utilizzo di un *software* antivirus aggiornato, di un *firewall* e la navigazione solo su siti *web* sicuri. Inoltre, devono evitare di fornire informazioni personali su siti *web* che non sembrano legittimi e di cliccare su *link* in *e-mail* o messaggi di testo sospetti.

Molte aziende e istituzioni finanziarie hanno implementato sistemi di sicurezza avanzati per proteggere i loro siti *web* dal *pharming*, come l'autenticazione a più fattori e la crittografia dei dati sensibili. Tuttavia, è importante che gli utenti continuino a

essere vigili e a seguire le buone pratiche di sicurezza per proteggere le loro informazioni personali¹⁸⁵.

3.2 Dalla *cybersecurity* al *cybercrime*: criminalità informatica

Dopo aver introdotto la *cybersecurity*, nonché le principali e più comuni tipologie di attacchi informatici¹⁸⁶, è opportuno analizzare come i continui progressi in ambito informatico e tecnologico abbiano portato alla necessità di ampliare lo studio dei *cybercrimes*, condotte criminose che si configurano come il “rovescio della medaglia” dell’evoluzione digitale. La propagazione di queste condotte è riconducibile sia, quindi, ai progressi informatici, sia alla sempre maggior “analfabetizzazione digitale”¹⁸⁷.

Nel termine *cybercrime* vengono ricomprese sia le condotte che configurano la *cyber threat*¹⁸⁸ (letteralmente “minaccia”), cioè i reati informatici propri, sia condotte che si allontanano dal concetto di *cyberattack*, come i reati informatici impropri.

¹⁸⁵ Cfr. Lombardo, S., Pharming: cos’è, come funziona e i consigli per difendersi dalla truffa dei “siti-trappola”, 28/01/2020, in www.cybersecurity360.it, data ultima visualizzazione 26/01/2023

¹⁸⁶ V. Cap III par. 3.1 ss.

¹⁸⁷ L’Italia in Europa è il fanalino di coda per quanto concerne il grado di digitalizzazione dell’economia e della società, anche a causa della scarsa educazione tecnologica confermata dalla DAD durante il lockdown. Lo conferma l’edizione 2020 del rapporto europeo Desi. <https://globalb.it/alfabetizzazione-digitale/>, data ultima visualizzazione 16/02/2023.

¹⁸⁸ La *cyber threat* è definita come il «*complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia, in particolare, nell’azione di singoli individui o organizzazioni, statuali e non, pubbliche o private, finalizzate all’acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi*». Cfr. D.P.C.M del 17 febbraio 2017, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*, cit., art 2, lett. l).

Consiste, quindi, nell'utilizzo illecito dei sistemi e delle reti per commettere determinati reati quali la frode informatica, la violazione della *privacy*, il furto di dati ecc.

Il nostro ordinamento, fin dalla nascita di queste condotte, è stato dotato di un apparato legislativo che conferisca carattere penale a illeciti di questa natura, grazie alla Legge 23 dicembre 1993, n. 547 recante “*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*”, in seguito modificata dalla legge 48/2008¹⁸⁹.

Le prime manifestazioni di criminalità informatica si possono far risalire all'inizio degli anni Settanta con i *computer crimes*, questi riferiti a condotte aventi ad oggetto un sistema informatico o telematico, non aperto al pubblico¹⁹⁰. In questi casi il computer è lo strumento utilizzato per commettere il reato.

Successivamente, intorno agli anni Novanta, con l'apertura di Internet al pubblico, il concetto di criminalità informatica si è ampliato, andando a ricomprendere non più la sola lesione di uno strumento informatico (appunto *computer crimes*), ma qualsiasi condotta criminale riconducibile alla rete e ai computer e, quindi, commessa nel *cyberspace*: da qui il concetto di *cybercrime*.

Non esiste una definizione giuridicamente rilevante condivisa, dal momento in cui in questa fattispecie rientrano diverse tipologie di condotte potenzialmente in grado di colpire beni giuridici diversi. In ogni caso, è possibile ricondurre il termine *cybercrime* al “*reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema o colpendolo*”¹⁹¹.

¹⁸⁹ Legge 23 dicembre 1993, n. 547 recante “*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*”, modificata con L. 48/2008.

¹⁹⁰ V. Picotti, L., *Diritto penale e tecnologie informatiche*, Utet Giuridica, Milano, 2019, p. 47.

¹⁹¹ V. Enc. Onl. Treccani, in www.treccani.it, data ultima visualizzazione 27/01/2023.

Questa tipologia di reati differisce da quelli tradizionali soprattutto per le caratteristiche tipiche della realtà informatica: il *locus commissi delicti*¹⁹² e il *modus operandi*, sempre nuovo e in grado di offendere i diritti altrui.

3.2.1 Reati informatici nel diritto

Dopo aver fornito un quadro sulla *cybersecurity* e quelle che possono essere le conseguenze a livello criminale, appare quindi essenziale un costante aggiornamento della realtà giuridica in relazione al fenomeno della criminalità informatica, mediante una serie normative che tengano conto delle ciò che accade nel *cyberspace*, il quale, essendo uno spazio virtuale difficile da controllare, determina il fatto che anche la criminalità informatica non sia giuridicamente definita, nonostante essa sia disciplinata in molteplici norme sia italiane che europee.

In materia di *cybercrime*, si riconduce ai primi anni Novanta l'esigenza del legislatore italiano di inserire nell'ordinamento una normativa *ad hoc*: vengono, così, introdotte all'interno del Codice Penale nuove fattispecie criminali seguendo la *ratio* ravvisata nella necessità di fornire una tutela per le nuove forme di attacchi informatici a beni fino a quel momento protetti da altre norme del medesimo codice.

L'incalzante espandersi del crimine informatico, quindi, condusse dall'esigenza di estendere le previsioni codicistiche allora vigenti, quali truffa (art. 640 c.p.) e delitto di danneggiamento (art. 635 c.p.), a nuove fattispecie.

Con la suddetta legge 23 dicembre 1993 n. 547, vengono quindi introdotte nel Codice Penale nuove fattispecie di reato di natura informatica quali:

¹⁹² Il reato viene, qui, perpetrato all'interno della rete informatica globale, il *cyberspazio*.

- la frode informatica, disciplinata all'art. 640 *ter* c.p. e costruita in relazione alla fattispecie di truffa¹⁹³;
- le falsificazioni di documenti informatici, di cui all'art. 491 *bis* c.p.¹⁹⁴;
- le aggressioni all'integrità dei dati e dei sistemi informatici, tra cui il danneggiamento dei sistemi informatici¹⁹⁵ (art. 635 *bis* c.p.);
- l'accesso abusivo ad un sistema informatico o telematico, ai sensi dell'art. 615 *ter* c.p.¹⁹⁶;

¹⁹³ La frode informatica richiama quanto disposto in tema di truffa (art. 640 c.p.), tuttavia presentando differenze in merito all'elemento causale, dal momento in cui nel reato di frode informatica non si richiede l'induzione in errore della vittima, in quanto l'attività fraudolenta investe il sistema informatico della stessa. La condotta consiste nell'alterazione, comunque realizzata, del sistema informatico e dell'intervento, senza averne diritto, con qualsiasi modalità, su dati, informazioni, programmi di un sistema informatico, in www.brocardi.it, data ultima visualizzazione 16/02/2023.

¹⁹⁴ La norma in esame prevede che, se la legge attribuisce efficacia probatoria ad un documento informatico, le condotte di falsità trovano applicazione. Quindi, a prescindere da un supporto cartaceo, il legislatore prevede la consumazione dei reati di falsità sin dal momento in cui i documenti predetti vengano inseriti in un registro informatico, o comunque trasmessi telematicamente, in www.brocardi.it, data ultima visualizzazione 16/02/2023.

¹⁹⁵ In questo contesto il bene giuridico tutelato è il patrimonio, in relazione a dati o programmi informatici altrui. La condotta che viene qui descritta riproduce quella del fatto illecito *ex art.* 2043 c.c., con la differenza riguardante la delimitazione dell'oggetto del danno che nel delitto in esame deve necessariamente essere un programma informatico o suoi dati e l'elemento soggettivo, limitato al dolo e non anche alla colpa, in www.brocardi.it, data ultima visualizzazione 16/02/2023.

¹⁹⁶ Il seguente articolo dispone che i beni giuridici oggetto di tutela in questo caso sono la riservatezza informatica e la indisturbata fruizione del sistema informatico da parte del gestore. La norma punisce due condotte: l'accesso non autorizzato in un sistema informatico o telematico protetto; il mantenimento in esso contro la volontà de gestore, in www.brocardi.it, data ultima visualizzazione 16/02/2023.

- la diffusione abusiva di codici di accesso a sistemi informatici prevista all'art. 615 *quater* c.p.¹⁹⁷.

L'introduzione della L. 547/1993 ha suscitato nel tempo diverse critiche¹⁹⁸, pur portando alla sottoscrizione della Convenzione di Budapest del 2001 sulla criminalità informatica¹⁹⁹, che costituisce il primo tentativo di "armonizzazione degli elementi fondamentali delle fattispecie di reato previste dai singoli ordinamenti interni e nel

¹⁹⁷ In questo caso il bene giuridico oggetto di tutela è la riservatezza informatica e la indisturbata fruizione del sistema informatico da parte del gestore. L'art. 615-*quater* punisce una condotta prodromica alla commissione del delitto di cui all'articolo precedente, sanzionando infatti la detenzione o la messa a disposizione di apparecchiature in grado di infrangere i presidi posti a tutela del "domicilio informatico altrui", in www.brocardi.it, data ultima visualizzazione 16/02/2023.

¹⁹⁸ Picotti, L., Commento all'art. 3 della legge n. 547 del 1993, in *Leg. pen.*, 1996, 71; Garrapa, N., *Internet e diritto penale: tra lacune legislative, presunte o reali, panorami transnazionali, analisi de iure condito e prospettive de iure condendo*, in *Diritto & Diritti*, 1999; Fondaroli, D., *Osservazioni intorno ad alcune delle norme contenute nella recente normativa italiana sui computer crimes*, in Sola, Fondaroli, D., (a cura di), *La nuova normativa in tema di criminalità informatica: alcune riflessioni*, Bologna, 1995, 20 ss.

¹⁹⁹ La Convenzione di Budapest definisce i termini più ricorrenti in materia di crimine informatico e nel mondo del *web* in genere. Sono diversi i motivi e gli obiettivi che hanno condotto alla Convenzione di Budapest: innanzitutto il carattere trans-nazionale del cosiddetto *cybercrime*, il crimine informatico. Il soggetto che realizza la condotta criminosa generalmente agisce tramite un *personal computer* e, a partire da quel momento, "l'azione telematica viene realizzata attraverso la connessione fra sistemi informatici distanti fra loro, per cui gli effetti della condotta possono esplicarsi in un luogo diverso da quello in cui l'agente si trova ad operare"; in secondo luogo, si è positivamente il bisogno di armonizzare i diversi quadri normativi vigenti nei diversi Paesi, nel tentativo di uniformare ed avvicinare il più possibile le legislazioni, gli strumenti applicativi, i controlli e, una parola l'effettività della tutela penale. Cfr. Manzari, M., *La convenzione di Budapest, l'alba di una normativa di contrasto efficace al cybercrime*, in *I reati informatici e la convenzione di Budapest*, bptm, 2021, <https://www.bptmavvocati.it/portfolio/i-reati-informatici-e-la-convenzione-di-budapest/>, data ultima visualizzazione 16/02/2023.

dotare i singoli Paesi di una normativa efficace per lo svolgimento delle indagini ed il perseguimento dei crimini correlati all'area informatica"²⁰⁰.

Con l'entrata in vigore della Convenzione di Budapest, il legislatore italiano si è dovuto adattare alle norme elaborate a livello europeo, mediante operazioni particolarmente complesse, arrivando all'approvazione della Legge 18 marzo 2008, n. 48 di ratifica della Convenzione di Budapest, con l'obiettivo di tutelare *“il rispetto del principio di proporzionalità, onde evitare di configurare incriminazioni caratterizzate da livelli sanzionatori che avrebbero potuto cagionare all'individuo ed alla società danni sproporzionatamente maggiori dei vantaggi ottenuti con la tutela dei beni e dei valori offesi dalle predette incriminazioni”*²⁰¹.

3.3 Cyberattacchi e Covid-19: virus a confronto

La pandemia da Covid-19 ha portato ad un aumento degli attacchi informatici in tutto il mondo, creando notevole incertezza, ansia e un drastico cambiamento nel nostro modo di vivere. Sono state sfruttate la paura e la confusione causate dalla pandemia per aggredire sistemi vulnerabili e rubare informazioni sensibili.

In particolare, per i *cybercriminali* è stato molto facile effettuare attacchi mediante la creazione di messaggi o siti *web* falsi che riproducevano l'aspetto di quello delle fonti ufficiali. In questa maniera è risultato semplice indurre le vittime in inganno, soprattutto nel momento in cui le restrizioni introdotte con il *lockdown* hanno intensificato l'utilizzo della tecnologia e della rete Internet.

Uno dei principali obiettivi degli attacchi informatici durante la pandemia è stato l'ambiente sanitario. Questo settore è particolarmente vulnerabile agli attacchi

²⁰⁰ Scognamiglio, P., *Criminalità informatica. Commento organico alla Legge 18 marzo 2008, n. 48*, Napoli, 2008.

²⁰¹ *Ibidem*.

informatici, come il già citato attacco *ransomware* “*WannaCry*”²⁰² che ha messo in ginocchio il Servizio sanitario nazionale nel 2017²⁰³.

Un attacco che ha sfruttato la vulnerabilità e la sensibilità della popolazione durante la pandemia da Covid-19 è stato “*Ginp*”, un *mobile banking trojan* che garantiva di visualizzare la posizione delle persone risultate positive al Covid-19 nelle vicinanze, tramite l’installazione di un’applicazione apparentemente utile, ma che al suo interno conteneva il *trojan*, la quale chiedeva un piccolo contributo di 75 centesimi con la promessa di mostrare la posizione delle persone positive nelle vicinanze. Una volta che la vittima inseriva i dati della carta per effettuare il pagamento, questi entravano in possesso dei criminali informatici²⁰⁴.

In generale, è stato registrato un aumento delle minacce informatiche contro organizzazioni italiane, soprattutto in ambito sanitario e governativo a causa della pandemia da Covid-19:

- 50 le minacce gravi rilevate e per le quali il Centro nazionale per le infrastrutture critiche opera nell'ambito della Postale, ha inviato *alert*, 45 quelle rivolte al settore sanitario, particolarmente esposto nella pandemia da *Coronavirus*;
- aumentate del 600% le mail di *phishing* legate al Covid, che invitano a scaricare contenuti apparentemente in tema ma che in realtà nascondono *malware* o *software* "maligni";

²⁰² V. par. 3.1.1.2.

²⁰³ Pranggono, B., Abdullahi, A., *COVID-19 Pandemic Cybersecurity Issues*, Internet technology letters, vol. 4 n. 2, 2021.

²⁰⁴ V. Taristano, P., *Ginp, il trojan Android che finge di segnalare i contagiati da Coronavirus*, 25/03/2020, in www.cybersecurity360.it, data ultima visualizzazione 29/01/2023.

- 28 le aziende che hanno denunciato di aver subito frodi informatiche, per circa 25 milioni²⁰⁵.

3.3.1 Danni subiti dalle aziende: strategie e modelli organizzativi per le imprese

Le organizzazioni, sia piccole e medie imprese (PMI) sia le multinazionali, hanno dovuto adattarsi alla richiesta di lavoro a distanza in modo rapido e su larga scala.

Passando ad un ambiente *online*, le aziende e gli enti pubblici hanno implementato il modello di *business* del lavoro da casa (cd. *smart working*), diventato la nuova normalità²⁰⁶. Esso aumenta i vettori di attacco e i rischi per i dati interni, poiché implica l'obbligo per i dipendenti di utilizzare i propri dispositivi personali e le proprie reti domestiche, che nella maggior parte dei casi non sono protette per natura e non dispongono delle misure di sicurezza standard industriali richieste. È importante, quindi, per le aziende attuare strategie e modelli organizzativi aziendali per la *cybersecurity* al fine di prevenire attacchi informatici²⁰⁷.

L'approccio del legislatore, attraverso la Direttiva 1148/2016 (NIS), il Regolamento EU 679/2016 (GDPR) e il decreto-legge 105/2019 sul Perimetro di Sicurezza Nazionale, è di indirizzare verso la scelta di misure di sicurezza più efficienti per difendersi dagli attacchi informatici.

²⁰⁵ <https://www.interno.gov.it/it/notizie/cybercrime-aumento-durante-lockdown>, data ultima visualizzazione 5/02/2023.

²⁰⁶ Secondo i dati ISTAT prima della pandemia solo il 3,6% delle amministrazioni era organizzato per lo *smart working*, passato al 58,9% nel 2020, www.istat.it.

²⁰⁷ Brotherston, V., L., Berlin, A., Viscardi, R., *La sicurezza dei dati e delle reti aziendali. Tecniche e best practice per evitare intrusioni indesiderate*, O'Reilly, 2018.

È innegabile che il progresso della tecnologia abbia e stia ancora rendendo difficile trovare una soluzione in assoluto in grado di evitare e contrastare gli attacchi informatici.

Per cui, servono soluzioni all'avanguardia e sempre aggiornate al fine di contrastare questo fenomeno sempre più difficilmente controllabile.

Ogni azienda deve essere in grado di individuare i propri "punti deboli" nel sistema informativo, analizzando le minacce per studiare e valutare il livello di difesa da adottare.

In sintesi, la pandemia da Covid-19 ha portato ad un aumento significativo degli attacchi informatici, sfruttando la paura e la confusione causate dal *virus* per aggredire sistemi vulnerabili e rubare informazioni sensibili. Inoltre, anche la diffusione dello *smart working* ha aumentato il rischio di *cyber* attacchi, tuttavia, con una combinazione di misure di sicurezza adeguate, formazione dei dipendenti e attenzione alle ultime minacce informatiche, le aziende possono proteggersi efficacemente.

La sicurezza informatica, quindi, non è un problema che può essere risolto una volta per tutte, ma richiede un impegno costante e un'attenzione continua per mantenere i sistemi al sicuro. Solo con una strategia di sicurezza informatica completa e all'avanguardia le aziende possono essere in grado di affrontare le sfide sempre maggiori che si presentano loro.

CONCLUSIONE

Questo lavoro non ha avuto la pretesa di affrontare in maniera capillare e onnicomprensiva il vasto argomento di cui si è occupato, ma solo quello di fornire a chi legge alcuni elementi da cui partire per approfondire la ricerca.

In questo elaborato sono stati enunciati i più rilevanti pericoli cui si espone l'utente che accede alla rete e al *cyberspace*. Taluni sono di natura tecnica e per questi sono stati forniti alcuni strumenti utili a restringere il campo di azione di coloro che minacciano i dati. Altri invece, più subdoli e meno facili da individuare, sono di natura psicologica e inducono il soggetto a compiere una o più azioni attraverso la suggestione, che può essere più o meno innocua.

In questo contesto, perciò, si manifesta tutto il *vulnus* del sistema, che non riesce a garantire totale protezione nei confronti dei soggetti e delle notizie che veicola. Spesso può accadere che, attraverso le maglie della legislazione, possa sfuggire la punibilità di chi mira ad eludere le norme ed ha come intento la captazione di notizie e informazioni di carattere sia personale che economico, allo scopo di truffa o di incidere sulla sfera della libertà decisionale, attraverso la manipolazione.

Si rileva inoltre che in un mondo ormai globalizzato è particolarmente difficile riuscire ad ottenere un sistema di norme di natura penale a carattere universale che possa garantire un'efficace rete di protezione.

Tutto questo conduce a considerare che è ancora *in fieri* il lavoro del legislatore, che deve tendere sempre più all'affermazione del principio di universalità delle norme penali nell'ambito di cui ci siamo occupati nella presente trattazione.

Anche dal punto di vista della conoscenza e/o conoscibilità del pericolo cui vengono esposti i soggetti nel momento in cui li si manipola, poco è stato fatto nell'ambito dell'educazione e della formazione degli utenti dei servizi: le tecniche manipolatorie utilizzate nelle teorie sopra esposte, come ad esempio il *nudge*, non sono conosciute dalla maggioranza di chi accede alla rete, in un contesto in cui si dovrebbe agire in

modo da prevenire i danni derivanti dalla pubblicità, dalle immagini subliminali e da altre forme di induzione di bisogni.

Occorrerebbe perciò agire sui due fronti: prevenire, attraverso una formazione ed informazione capillare, in modo tale da rendere il navigante del *web* consapevole dei rischi cui potrebbe esporsi, ma soprattutto normare in maniera uniforme, su tutta la rete, il sistema degli annunci e addivenire poi, in un momento successivo, alla stesura di un codice di comportamento transnazionale, che contempra in modo uniforme i reati e stabilisca altrettanto univocamente i mezzi di repressione e le conseguenti sanzioni.

In conclusione, il presente lavoro di tesi ha cercato di esplorare il fenomeno dell'ingegneria sociale e la sua relazione con la *cybersecurity*, concentrandosi sulla comprensione delle tecniche utilizzate dagli aggressori per manipolare il comportamento umano e sulle strategie di difesa per proteggere gli individui e le organizzazioni da questi attacchi.

Il primo capitolo ha fornito una panoramica generale sull'ingegneria sociale, introducendo il concetto di Roscoe Pound e fornendo un'analisi circa il paternalismo libertario e la teoria del *nudge*, corredata da esempi. Inoltre, un aspetto che generalmente viene trascurato riguarda il tema della giuridicità del *nudge* a cui, nella stesura dell'elaborato, è stata posta particolare attenzione. In questo capitolo è stata sottolineata poi l'importanza della comprensione della psicologia umana per prevenire e contrastare gli attacchi di ingegneria sociale.

Successivamente, nel secondo capitolo l'attenzione si è spostata sul ruolo delle emozioni nella comprensione del comportamento umano e sulle neuroscienze in genere. Attraverso l'analisi di alcune ricerche in ambito neuroscientifico e lo studio di alcuni casi giurisprudenziali, si è cercato di comprendere i meccanismi cognitivi ed emotivi che rendono gli individui suscettibili agli attacchi di ingegneria sociale. Nel corso di questo capitolo è stata sottolineata l'importanza di una maggiore interazione tra la sicurezza informatica e le neuroscienze al fine di sviluppare strategie più efficaci

per proteggere gli individui dai rischi della rete, oltre al ruolo che le neuroscienze hanno nella teoria giuridica e in particolar modo la relazione tra esse e il diritto penale. Infine, nel terzo capitolo è stato affrontato il tema della *cybersecurity* e della responsabilità in rete. Dopo aver fornito una panoramica sul *cyberspace* (dall'attribuzione del termine a Gibson all'avvento di Internet) e sulle principali tipologie di attacchi informatici, l'attenzione si è spostata sull'importanza che i continui progressi in campo informatico e tecnologico hanno portato in materia penale e, quindi, allo studio dei *cybercrimes*. Il capitolo è stato concluso con un'analisi circa il crescente aumento delle minacce cibernetiche durante la pandemia da Covid-19, con un *focus* sulla vulnerabilità delle persone e delle organizzazioni a seguito del sempre maggior utilizzo della rete.

In generale, la ricerca ha voluto dimostrare l'importanza di una maggiore consapevolezza dei rischi di ingegneria sociale e del loro impatto sulla sicurezza informatica, sottolineando la rilevanza di una maggiore collaborazione tra i professionisti della sicurezza informatica e gli esperti delle neuroscienze per sviluppare strategie più adeguate a proteggere la società dalla manipolazione psicologica.

Infine, è doveroso sottolineare come questo elaborato rappresenti solo un piccolo passo verso la comprensione dell'ingegneria sociale e della sua relazione con la *cybersecurity*. Sono ancora molte le domande aperte e gli argomenti che possono essere affrontati, con la speranza che questo lavoro possa contribuire nel suo piccolo ad una maggiore consapevolezza e ad un miglioramento delle strategie di difesa contro gli attacchi informatici.

Alla luce di quanto sopra esposto, secondo la scrivente, sarebbe opportuno addivenire ad un capillare sistema di trattati internazionali con la finalità di redigere dei codici di

comportamento univoci valevoli per tutto il mondo virtuale: in questo panorama sarebbe quindi garantita la certezza della repressione dei reati informatici che assumono sempre più rilevanza nell'ordinamento giuridico internazionale.

BIBLIOGRAFIA

Amato Mangiameli, A. C., *Diritto e cyberspace: appunti di informatica giuridica e filosofia del diritto*, Torino, Giappichelli, 2000

Aterno, S., *Sicurezza informatica: aspetti giuridici e tecnici*, Pacini Giuridica, Pisa, 2022

Baggio, M., & Motterlini, M., *Negare il rischio: irrazionalità, salute e architettura delle scelte*, Sistemi intelligenti, 29(2), 2017

Barker, J., *The human nature of cybersecurity*, Educause Review 54, n. 2, 2019

Bault, N., Rusconi, E., *I Meccanismi Neurocognitivi Del Nudge*, Giornale italiano di psicologia, 2020

Bertolino, M., *L'imputabilità penale fra cervello e mente*, in Di Giovine, O., (a cura di), *Diritto penale e neuroetica*, Padova, Cedam, 2013

Bianchi A., Gulotta G., Sartori G., *Manuale di neuroscienze forensi*, Giuffrè Editore, 2009

Bianchi, A., *Neuroscienze e diritto: spiegare di più per comprendere meglio*, in AA.VV., *Manuale di neuroscienze forensi*, Milano, 2009, XII

Bogliacino, F., Veltri, G., Codagnone, C., *Nudge, ovvero la "spinta gentile"*, Aggiornamenti Sociali, 2016

Boniolo, G., Rebba, V., *Il Nobel per l'economia 2017 a Richard Thaler: l'idea del nudging per le politiche sanitarie. Politiche Sanitarie*, 18(3), 2017

Breda, F., Barbosa, H., Morais, T., *Social Engineering and cybersecurity*, 2017

Brotherston, V., L., Berlin, A., Viscardi, R., *La sicurezza dei dati e delle reti aziendali. Tecniche e best practice per evitare intrusioni indesiderate*, O'Reilly, 2018

Caruana, F., Viola, M., *Come funzionano le emozioni*, Il Mulino, Bologna, 2018

Chece, D., M., *La filosofia delle emozioni dal pragmatismo alle neuroscienze*, in *Ragion pratica, Rivista semestrale*, 2/2021

Codognotto, S., Sartori, G., *Neuroscienze in tribunale: la sentenza di Trieste*, in *Sistemi intelligenti, Rivista quadrimestrale di scienze cognitive e di intelligenza artificiale*, 2/2010

Conteh, N., Y., Schmick, P., J., *Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks*, *International Journal of Advanced Computer Research*, vol. n. 6, 2016

Cuomo, L., Razzante, R., *La nuova disciplina dei reati informatici*, Torino, Giappichelli, 2007

Dal Checco, P., *Il ransomware Wannacry infetta PC non aggiornati: ospedali ed enti pubblici a rischio*, 2017

Damasio, A. R., *Descartes' Error: Emotion, Reason, and Human Brain*, New York, Penguin; trad. It. *L'errore di Cartesio. Emozioni, ragione e cervello umano*, Adelphi, Milano, 1995

Damasio, A., *Alla ricerca di Spinoza. Emozioni, sentimenti e cervello*, Adelphi, 2003

Darwin, C., *The Expression of the Emotions in Man and Animals*, Penguin Classics, 2005

Di Giovine O., *Ripensare il diritto penale attraverso le (neuro-)scienze?*, Giappichelli, Torino, 2020

Di Giovine, O., *Un diritto penale empatico?*, Torino, Giappichelli, 2009

Fagioli, S., *Filosofia retorica e logica argomentativa in Aristotele*, Torino, Giappichelli, 2022

Farano, A., *Emozioni e teoria del giudizio: una prima ricostruzione*, BioLaw Journal, Rivista Di BioDiritto, 2020

Farano, A., *Garantismo penale ed epistemologia giudiziaria: considerazioni a margine di un caso di lie detection*, in Marzocco, V., (a cura di), *La dignità in questione*, Torino, Giappichelli, 2018

Farano, A., *La responsabilità giuridica alla prova delle neuroscienze*, Bari, Cacucci Editore, 2018

Fiandaca, G., Musco, E., *Diritto penale. Parte generale*, Il Mulino, Bologna, 2010

Filindeu, M. T., *Colpevolezza e neuroscienze: prospettive di un confronto dialogico*, in *Itinerari di Diritto Penale*, Giappichelli, Torino, 2022

Flick, G., M., *Neuroscienze e diritto*, in Sangalli, S., (a cura di), *Futuro e responsabilità. Secondi dialoghi di pratica etica*, Luiss Academy, 2015

Flor, R., *Cybersecurity ed il contrasto ai cyber-attacks*, in *DIRITTO DI INTERNET*, n.3, 2019

Forza, A., Menegon, G., Rumiati, R., *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2011

Fuselli, S., *Le emozioni nell'esperienza giuridica: l'impatto delle neuroscienze*, in Palazzani, L., e Zannotti, R., (a cura di), *Il diritto nelle neuroscienze. Non "siamo" i nostri cervelli*, Torino, Giappichelli, 2013

Galletti M., Vida S., *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, Roma, 2018

Gibson, W., *Neuromance*, Ace, 1994, trad. ita. *Neuromante*, Cossato, G., Sandrelli, S., Milano, Mondadori, 2017

Harries, D., *Narrative Mapping of Cyberspace. Context and Consequences*, in Ramírez Luis, J., M., García-Segura, A., (A cura di), *Cyberspace Risks and Benefits for Society, Security and Development*, Berlino, Springer, 2017

Jouvenal, R. *Roscoe Pound e il diritto*. Il Politico, vol. 29, n. 3, 1964

Kahneman, D., *A perspective on judgment and choice: mapping bounded rationality*, Am. Psychol, 2003

Kahneman, D., Knetsch, J. L., Thaler, R. H., *The endowment effect, loss aversion, and status quo bias*, Journal of Economic perspectives, 1991

Kahneman, D., *Pensieri lenti e veloci*, Edizioni Mondadori, Milano, 2012

Kahneman, D., Tversky, A., *On the reality of cognitive illusions*, 1996

Kahneman, D., Tversky, A., *Prospect theory: An analysis of decision under risk*, in Handbook of the fundamentals of financial decision making: Part I, 2012

Lana, A., *I love You, venti anni fa il primo virus informatico che ha messo il mondo in ginocchio*, 4/05/2020

Lattanzi, N., *Verso la convergenza tra neuroscienze e intelligenza artificiale*, in *Nuova Antologia. Rivista di lettere, scienze ed arti*, Gennaio-Marzo 2020, Vol. 624, Fasc. 2293, Edizioni Polistampa, Firenze, 2020

Lombardo, S., *Pharming: cos'è, come funziona e i consigli per difendersi dalla truffa dei "siti-trappola"*, 2020

Martino, L., *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, Fascicolo 1/2018

Maurer, C., *La Theorie des Gefühls hegeliana in dialogo con le recenti teorie sulle emozioni*, Rivista internazionale di filosofia e psicologia, 2017, vol. 8, n. 1

Mensi, M., Falletta, P., *Il diritto del web*, Padova, Cedam, 2018

Mensi, M., *La sicurezza cibernetica*, in Mensi, M., Falletta, P., *Il diritto del web*, Cedam, 2018

Mezzalama, M., Liroy, A., Metwalley, H., *Anatomia del malware*, in Riv. Mondo Digitale, 47/2013

Pellegrini S., *Il ruolo dei fattori genetici nella modulazione del comportamento: le nuove acquisizioni della biologia molecolare genetica*, 2009, in Bianchi, A., Gulotta, G., e Sartori, G., (a cura di), *Manuale di neuroscienze forensi*, Milano, Giuffré

Picotti, L., *Diritto penale e tecnologie informatiche*, Utet Giuridica, Milano, 2019

Pranggono, B., Abdullahi, A., *COVID-19 Pandemic Cybersecurity Issues*, Internet technology letters, vol. 4 n. 2, 2021

Pravettoni, G. *La mente impressionabile: come utilizzare le «spinte gentili» per fare scelte salutari*, in Giornale italiano di psicologia, Rivista trimestrale, 2/2020

Rebonato, R., *Taking Liberties: A Critical Examination of Libertarian Paternalism*, Palgrave MacMillan, London, 2012

Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019

Romeo, F., *Lezioni di logica ed informatica giuridica*, Torino, Giappichelli, 2012

Sammicheli, L., Sartori, G., *Neuroscienze giuridiche: i diversi livelli di interazione tra diritto e neuroscienze*, in Bianchi, A., Gulotta, G., Sartori, G., (a cura di), *Manuale di neuroscienze forensi*, Milano, 2009

Savadori, L., *Nudge: opportunità o moda passeggera?*, *Giornale italiano di psicologia*, 2020

Scardovi, G., *Mondo che genera mondo: memoria, codice, cyberspazio*, in *Politica & Società*, *Periodico di filosofia politica e studi sociali* 1/2018

Scognamiglio, P., *Criminalità informatica. Commento organico alla Legge 18 marzo 2008, n. 48*, Napoli, 2008

Sharot, T., *The Optimism Bias: Why We're Wired to Look on the Bright Side*, London, Robinson, 2012

Thaler, R., Sunstein, C., Balz, J., *The Behavioral Foundations of Public Policy*. Princeton, New Jersey, Princeton University Press, 2013

Thaler, R., Sunstein, C., *Nudge: La spinta gentile*. Milano, Feltrinelli Editore, 2009

Tversky, A., Kahneman, D., *The framing of decisions and the psychology of choice*, *science*, 211(4481), 1981

V. Taristano, P., *Ginp, il trojan Android che finge di segnalare i contagiati da Coronavirus*, 2020

Viale, R., Macchi, L., *Analisi comportamentale delle politiche pubbliche*, Il Mulino, Bologna, 2021

Witte, K., Allen, M., *A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns*, *Health Education & Behavior: The Official Publication of the Society for Public Health Education* 27, 2000

GIURISPRUDENZA

Cass. sez. I 11 ottobre 1995, in CED Cassazione n. 203651

Cass. sez. I 5 dicembre 1997, in Cass. Pen., 1999, p. 156 in Riv. it. Med. Leg., 1999, p. 341 in CED Cassazione n. 209382

Cass. Sez. Un., 8 marzo 2005, n. 9163, Raso

Cass., sez. I, 22 aprile 1997

Cass., sez. I, 3 marzo 1993

Cass., sez. V, 5 aprile 1990, in Cass. pen., 1991, I, p. 1565

Cass. Pen. Sez. IV, 13 dicembre 2010 (17 settembre 2010), n. 43786 - Pres. Marzano - Est. Blaiotta - P.M. Delehayé (diff.) - Cozzini e altri

Corte di Assise di Appello di Trieste, R.G.N.R 1685/2007, sent. 18 settembre 2009, n. 5, in *Rivista penale*, 2010, con nota di Forza A., *Le neuroscienze entrano nel processo penale*. Riconosce tuttavia che le neuroscienze «*possono contribuire sull'iter decisionale del giudice aprendogli nuovi orizzonti di pensiero*», già Corte d'Assise d'Appello di Venezia, 14.8.2008, Favaro

Tribunale di Como, R.G.N.R 4948/09, sent. 20 maggio 2011, n. 536, Albertani, in *Rivista italiana di medicina legale*, 2012, con nota di MESSINA G., *I nuovi orizzonti della prova (neuro) scientifica nel giudizio sull'imputabilità*

Tribunale di Venezia, G.i.p. dott.ssa Roberta Marchiori, 24 gennaio-8 aprile 2013,
sent. n. 296