UNIVERSITÀ DEGLI STUDI 'SAPIENZA' DI ROMA
ACCADEMIA INTERNAZIONALE DI FILOSOFIA DEL DIRITTO

STUDI DIRETTI DA
L. AVITABILE - G. CARCATERRA - A. CERRI
P. MARCONI - F. MODUGNO - A. RIVERA LLANO - B. ROMANO

M. INNOCENZI - B. LEUCADITO - G. PETROCCO

IL DIRITTO TRA DIGITALE ED ESISTENZIALE

G. GIAPPICHELLI EDITORE – TORINO

MARIALUISA INNOCENZI

Diritto e diritti in rete.
Una fenomenologia degli attacchi cibernetici

Avvio

Con sguardo rivolto all'incremento degli attacchi *virali*, quest'itinerario di ricerca concentra l'attenzione sugli esiti delle azioni criminose in rete, lasciando cogliere come queste si riverberano in ambiti e prospettive non distanti dalla giuridicità, investendo l'esistenza umana e i fenomeni ad essa collegati – libertà, uguaglianza, sicurezza, imputabilità [1] –.

L'accesso incontrollato in rete e l'immensa quantità di contenuti condivisi su *internet* lasciano intravedere come il principio di uguaglianza sia, costantemente, minacciato dall'instaurarsi di rapporti di sproporzione tra chi ha le competenze tecniche per acquisire ed elaborare i dati e chi è destinatario di tale abilità [2].

Nella storia dell'umanità è sempre stato chiaro chi fosse il dominante e chi l'asservito. Le lotte per l'affermazione dei diritti si radicano, da sempre, in una dimensione di disuguaglianza tra una *élite* di potenti e il resto del genere umano che, oggi, appare immerso in una fluttuazione virtuale, raramente illuminata da scelte consapevoli e responsabili [3].

In questa prospettiva, non è solo la *dromocrazia* a minacciare l'integrità delle condotte compiute nello spazio cibernetico, è la crescente disponibilità delle informazioni a trasformare gli *users* in risorse da sorvegliare, attaccare e veicolare verso obiettivi sempre più lontani dall'orizzonte giuridico [4].

---

[1] Cfr. L. AVITABILE, *Legalità e giustizia. I Feuerbach e Radbruch*, Torino, 2021; B. ROMANO, *Civiltà dei dati. Libertà giuridica e violenza*, in *Opera Omnia*, Torino, 2021.

[2] Cfr. B.-C. HAN, *La società senza dolore. Perché abbiamo bandito la sofferenza dalle nostre vite*, Torino, 2021; ID., *L'espulsione dell'altro*, Milano, 2017, pp. 49-51; E. MOROZOV, *L'ingenuità della rete. Il lato oscuro della libertà di internet*, Torino, 2011.

[3] Cfr. B. ROMANO, *Civiltà dei dati. Libertà giuridica e violenza*, cit., p. 10.

[4] Il sistema della produzione e condivisione delle informazioni è radicalmente mutato: se, fino a qualche tempo fa, gli *users* apparivano come ricettori passivi di dati, oggi sul *web* si impone una nuova interattività. I contenuti sono

Oggi, un nuovo potere si impone. Pirati informatici, persone in carne ed ossa, programmano sistemi in grado di eseguire attività intrusive – a scopo estorsivo – che cristallizzano l'odierna supremazia *tecnocratica*, elevandola a centro di comando di nuove forme di violenza.

Si avvia, da qui, un'opera di riflessione sulla condizione contemporanea che apre alcuni itinerari per una interpretazione del diritto attenta all'attuale processo di cambiamento della giuridicità e dell'intera esistenza – più specificamente della persona, non incontrata come soggetto di diritto ma trattata come *nodo di trasmissione* e *stazione ricevente*[5].

Le considerazioni proposte trattano i temi del diritto e della giustizia in rete, nella consapevolezza che il sapere giuridico e quello informatico sono l'uno essenziale all'altro.

Le tecnologie rappresentano, certamente, un'immensa ricchezza, eppure non è possibile tralasciare alcune considerazioni sulla comparsa di nuove dinamiche sociali ed economiche che spingono i capitalisti del digitale ad acquisire informazioni utili per accrescere il potere economico di pochi, a dispetto dell'intera umanità[6].

La rete, non più terra di mezzo, si manifesta, infatti, come un insieme di nodi interconnessi, membri di una *cyber*-società che a tratti sembra riproporre i 'profili' di uno stato di natura *à la Rous-*

---

generati, condivisi e ri-condivisi da migliaia di naviganti. In Italia, attualmente, si contano oltre 41 milioni di utenti attivi sui *social* (dal *Digital 2021. Global overview report*). Il termine *social-network* individua siti *internet* o piattaforme tecnologiche che consentono agli utenti di interagire e condividere contenuti fotografici, audio, video, testi. Inizialmente considerati dispositivi, a breve durata, per attività ricreative, l'utilizzo dei *social* ha sollevato questioni complesse legate a fenomeni di *cyberbullismo*, *cyberterrorismo*, *grooming*, *fake news*, revenge porn, violazione dati personali, etc. …, alimentati dall'*ipercomunicazione digitale* che frastorna le relazioni umane convertite, ormai, in connessioni *internettiane*, veloci, economiche e sempre accessibili. La rete, asse portante dell'odierna civiltà digitale, pone problemi e questioni giuridiche nuovi, con i quali il giurista è chiamato a confrontarsi. Cfr. P. GALDIERI, *Il Diritto penale dell'informatica: legge, giudice e società*, Torino, 2021.

[5] B.-C. HAN, *La società senza dolore*, cit., p. 23.

[6] Cfr. S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Milano, 2019.

seau concepito, a volte, come *condizione di innocenza*, altre come *luogo gravido di pericoli*[7].

Muovendo dalla lettura di alcuni classici del pensiero, si discuterà il convincimento che giuristi, filosofi, scienziati non sono esonerati da un confronto sulla giuridicità, anzi diventa la chiave teorica per riproporre e affrontare un comune ambito di problemi sulla vita delle istituzioni giuridiche e degli individui che, concretamente, vivono ed agiscono nella contemporaneità.

Una domanda si pone sin dall'inizio. Nella nuova geografia di internet, il diritto agisce come *limite* normativo essenziale, oppure *limita* i progressi tecnologici?

La discussione chiede di mettere in questione i contenuti normativi istituiti dal legislatore, a partire dall'esplicitazione di *legge giuridica* come *ordine della legalità* che nulla ha a che vedere con le leggi della robotica e della cibernetica, spogliate delle domande sulla giustizia[8]. Questo ed altri quesiti fanno luce sulla centralità del fenomeno giuridico, declinato come diritto duttile, indeterminato ed elastico. Si prende distanza dall'idea che una norma scritta, autoritaria e rigida possa essere obbedita senza essere interpretata.

Si è sollecitati a considerare che, sin dalla sua prima apparizione, il diritto si manifesta come fenomeno esclusivo della relazionalità umana, non riducibile ad altri fenomeni come l'economia, la politica, la religione. Questi pur appartenendo all'ambito delle relazioni esistenziali incidono, nella concretezza dell'esistenza del singolo e della collettività, in modo diverso da come agisce la giuridicità.

Il *diritto* fa il suo ingresso nell'ambito della relazione intersoggettiva e, specificamente, in quelle modalità del relazionarsi in cui un *io* ed un *tu* si ritrovano l'uno nell'altro, senza perdersi in una condizione di isolamento che rischia di cancellare *l'originalità creativa*, esclusiva dell'essere umano[9].

---

[7] J.-J. ROUSSEAU, *Il contratto sociale*, Milano, 2018, p. 129 ss.

[8] Cfr. B. ROMANO, *Ingiustizia radicale e narcisismo*, Torino, 2021; ID., *Principi generali del diritto Principio di ragione e principio dialogico*, Torino, 2015.

[9] Cfr. L. AVITABILE, *Cammini di filosofia del diritto*, Torino, 2012.

Il rapporto uomo-diritto va considerato, nella situazione attuale, insieme al rischio di essere sostituito da dinamiche calcolanti che – come si va progressivamente esaminando – lasciano inevasa la questione del *giusto* e dell'*ingiusto*, legittimando l'esercizio della violenza [10].

Una discussione sulla condizione giuridica, comparativamente con altri fenomeni sociali, chiede di essere affrontata tenendo conto di quel che accade nel momento storico contemporaneo: l''utopico' processo di ibridazione tra reale e virtuale si è concretizzato, lasciando emergere una complessa e rinnovata dimensione che oltrepassa anche il mondo digitale.

Si apre un nuovo scenario che orienta le relazioni sociali verso spazi iperconnessi, fino a raggiungere il *metaverso* [11]: un luogo *metareale* che promette libertà e contenuti inesauribili, trasponendo l'essere umano in una dimensione ultra-virtuale, popolata da *avatar* tridimensionali che co-abiteranno in una geografia cibernetica senza precedenti, ma che si sottrae alla lentezza del *nomos* [12].

Nelle diversificate declinazioni del diritto, questo studio intende riprendere alcuni elementi centrali nel pensiero di Norbert Wiener e Paul Ricœur studiosi proiettati verso orizzonti speculativi diversi, eppure necessari per tornare a riflettere sul compito *dell'interpretazione giuridica* recepita non più come *arte* ma come *tecnica*, scontrandosi così con l'idea classica del diritto quale *ars boni et aequi* [13].

Il giurista, il filosofo, lo scienziato possono confinarsi nei loro

---

[10] B. ROMANO, *Civiltà dei dati. Libertà giuridica e violenza*, cit., *passim.*

[11] Coniato per la prima volta da Neal Stephenson, nel romanzo *Snow crash* (1992), questo neologismo sincratico formato dalla fusione delle parole *meta*, dal greco *oltre*, e *universo* rinvia all'idea di un mondo *oltre il virtuale*, dove rappresentazioni tridimensionali si muovono in spazi raggiungibili con caschi virtuali, *smart glasses*, guanti e tute tattili. La convinzione che i sistemi di realtà aumentata possano imporsi sull'esistenza umana lascia aperti numerosi interrogativi, chiedendo di affrontare la questione sia dal punto di vista sociale, etico ed economico, ma anche e soprattutto giuridico.

[12] Vd. B. ROMANO, *Dalla metropoli verso internet*, Torino, 2017, p. 73.

[13] Cfr. AA.VV., *Giuristi della 'Sapienza'. Questioni di filosofia del diritto*, Torino, 2015.

specifici terreni di ricerca regionalizzati secondo le diverse tecnicalità? Come si rapportano con le questioni connesse alla libertà, all'uguaglianza e alla giustizia?

Discutere di diritto – nella sua più significativa espressione di *diritti umani* – significa avvicinarsi alla diramazione tra giusto e ingiusto, legale e illegale, nella consapevolezza che non spetta alla scienza stabilire, in modo assoluto, i criteri in base ai quali operare una distinzione tra ciò che bene o male, lecito o illecito.

Occorre ricordare che il diritto si manifesta, fenomenologicamente, come rapporto mediato da un soggetto *super-partes*, custode della relazione giuridica, che ne impedisce lo scivolamento in una chiusa condizione di univocità [14].

Tappa fondamentale di questo cammino è l'analisi del concetto giuridico di responsabilità, nella sua accezione di *respondere criminibus* [15]. Nell'attuale contesto cibernetico, si scorge la visione di una *colpa senza responsabilità* che conduce ad esiti *de*responsabilizzanti [16], aprendo ulteriori domande sulla nozione di imputabilità.

In rete, responsabile è chi entra nella condizione del *responsum*, obbligando l'autore di un atto a risponderne?

Queste brevi considerazioni iniziali invitano a prendere atto che non è possibile compiere «un'opera di riflessione rinunciando ad acquisire la consapevolezza che […] la si compie nel mondo di oggi e non in un altro mondo» [17]: le riflessioni sull'essere umano, e dunque sul diritto, muovono proprio dall'analisi del vivere in società.

L'affermazione di Bruno Romano delinea la cornice argomentativa di queste pagine, nella direzione in cui si comprende che «non è dato agli esseri umani di esistere in un mondo diverso da quello proprio della loro esistenza di tutti i giorni» [18]: un'esistenza immersa in spazi affollati da tecnologie *intelligenti*, abilmente

---

[14] Cfr. B. ROMANO, *Relazione e diritto tra moderno e postmoderno*, in *Opera Omnia*, Torino, 2021.

[15] Cfr. CICERONE, *Le Catilinarie*, Milano, 1994.

[16] B. ROMANO, *Soggettività, diritto e postmoderno. Una interpretazione con Heidegger e Lacan*, Roma, 1988, p. 88.

[17] ID., *Civiltà dei dati. Libertà giuridica e violenza*, cit., p. 11.

[18] *Ibidem.*

convertite – attraverso strategiche attività di *hacking* – in forme di coercizione che rischiano di compromettere i principi di libertà, uguaglianza e dignità, asse portante di ogni civiltà democratica [19].

1. *Vulnerabilità sistemiche e diritto. Un'analisi del contesto contemporaneo*

«Nel nome della sopravvivenza sacrifichiamo volentieri tutto ciò che rende la vita meritevole di essere vissuta. Dinanzi alla pandemia, anche la radicale limitazione dei diritti fondamentali viene accettata senza discussioni» [20]. Queste parole di Han consentono di avviare una riflessione sui diritti universali ed incondizionati di ciascun essere umano – donna o uomo, cittadino o apolide –, chiamando filosofi, giuristi e scienziati a sviluppare i propri temi di ricerca in maniera originale e rigorosa, avendo attenzione all'attuale contesto sociale che registra un numero crescente di minacce virali.

Nei primi mesi del 2020, mentre la pandemia avvolgeva il mondo intero, solo in Italia, quasi 43 milioni di persone – tra queste tre milioni di *entry level* – sono rimasti in contatto *grazie* all'uso della rete che, se da un lato ha consentito la prosecuzione delle attività quotidiane, dall'altro ha accelerato l'evoluzione di nuove forme di violenza, fino a consolidare l'esigenza di adottare, in tempi brevi, misure di mitigazione, sempre più stringenti, essenziali sia a prevenire nuove aggressioni, sia a garantire il ripristino dei servizi violati [21].

La repentina transizione al digitale, veicolata dal virus – *specchio della nostra società* [22] –, ha inevitabilmente ridefinito abitudini e comportamenti, invaso la sfera relazionale e modificato le re-

---

[19] Cfr. R. MEGGIATO, *Imparare l'hacking*, Milano, 2018; K.D.W. MITNIC-L. SIMON, *L'arte dell'inganno*, Milano, 2013.

[20] B.-C. HAN, *La società senza dolore*, Torino, 2021.

[21] Attraverso lo studio dei fenomeni sociali ed economici più significativi, il rapporto *Censis* fornisce un quadro della sicurezza informatica nazionale, evidenziando le vulnerabilità strutturali dei sistemi informativi della nazione.

[22] B.-C. HAN, *La società senza dolore*, cit., p. 22.

gole sociali, dissolvendo gli ordinari luoghi di comunità, lavoro e formazione.

In bilico tra due poli complementari, fisico e digitale, la corsa salvifica verso una quotidianità *agile* ha progressivamente confinato gli esseri umani nel labirinto senza uscita del *world wide web*, attraversato da milioni di utenti alla ricerca di servizi e contenuti interattivi creati su misura per il navigante [23].

Conferenze, concerti e *pièce* teatrali sono diventati palcoscenici virtuali; gallerie, musei e mostre d'arte approdano in *streaming*. Alla pubblica piazza subentra la *piattaforma delle piattaforme* [24].

Ormai, anche lo spazio cibernetico appare totalmente riconfigurato, lasciando intensificare l'esigenza – prioritaria per il giurista positivo – di circoscrivere l'universo *cyber* entro i confini della legalità, nel tentativo di scongiurare il rischio che la rete si trasformi in un mondo senza legge.

Il *Rapporto Clusit sulla sicurezza ICT in Italia e nel mondo* mostra come lo scenario nazionale delle *cyber*-intrusioni sia profondamente mutato negli ultimi anni [25]. Gli attacchi informatici sono evoluti in qualità e quantità! La pericolosità e l'imprevedibilità dei rischi cibernetici impongono agli utenti di adottare condotte consapevoli e sicure.

---

[23] Una riflessione sui livelli di sicurezza in rete esige la chiarificazione dei concetti di *cyberspace* e *cyberthreat* ognuno dei quali, con una propria consolidata definizione, interessa il rapporto tra diritto e *cybersecurity*. Se da un lato, la fusione dei termini «cibernetica» e «spazio» ha contribuito a identificare uno *pseudo-luogo* in cui si interagisce grazie all'uso della rete; dall'altro la combinazione dei due termini – *cyber-threat* (minaccia) – rinvia ad una manovra di attacco verso un sistema informatico che persegue l'obiettivo di accedere, modificare, sottrarre e/o distruggere informazioni e dati. Norbert Wiener (1894-1964) matematico e statistico statunitense è, ancora oggi, ricordato come il padre della cibernetica.

[24] Cfr. B. ROMANO, *Civiltà dei dati. Libertà giuridica e violenza*, in *Opera Omnia*, cit., *passim*; M. CASTELLS, *Comunicazione e potere*, Roma, 2017.

[25] Il *report Clusit sulla sicurezza informatica ICT* mostra, periodicamente, l'andamento degli incidenti virtuali in Italia e nel mondo. L'incremento e la maggiore gravità d'impatto degli attacchi impone, infatti, un monitoraggio costante e attento. In particolare, nel primo semestre del 2021, rileva una crescita significativa di *attacchi gravi* nelle seguenti categorie: *Transportation/Storage* (+ 108,7%), *Professional Scientific Technical* (+ 85,2%) e *News & Multimedia* (+ 65,2%), seguite da *Wholesale/Retail* (+ 61,3%) e *Manufacturing* (+ 46,9%).

Avendo attenzione alla situazione attuale, i dati mostrano che gli *hackers* sfruttano strategie di intrusione multiformi, aprendo uno scenario marcato dall'accelerazione di alcune linee di tendenza verso una maggiore aggressività e cronicizzazione di azioni a matrice *non identificabile*, sfuggendo ad ogni forma di controllo[26].

In particolare, l'analisi degli attacchi conferma il proliferare di *azioni offensive* messe a segno utilizzando prevalentemente *malware*, tra i quali spiccano i sempre più evoluti ed efficaci *ransomware*[27] (*trojan horse crittografici*): quest'ultimi causano, nei computer infettati, l'inaccessibilità ai dati, subordinando il ripristino e la disponibilità dei *file* cifrati al pagamento di un riscatto[28].

La crisi pandemica ha evidenziato le vulnerabilità infrastrutturali dei servizi e sistemi digitali nazionali, minacciati da azioni intrusive sempre più sofisticate che costringono il legislatore ad ac-

---

[26] Si tratta di operazioni veicolate da strategie di attacco sconosciute (*unknown*) che non consentono di individuare né le vittime, né gli aggressori, né le cause dell'intrusione rendendo ancor più complesso il processo di attribuzione dell'attacco e della relativa responsabilità giuridica.

[27] Si veda il *Documento di Sicurezza Nazionale*, allegato ai sensi dell'art. 38, comma 1 *bis*, legge n. 124/2007 alla *Relazione Annuale al Parlamento*, p. 55: «Il complesso degli attacchi cibernetici rilevati nel 2020 ha confermato, in linea con quanto emerso nell'ultimo biennio, *l'hacktivismo* come matrice più ricorrente (71%), sebbene non si siano registrati, rispetto al 2019, significativi scostamenti nel numero di azioni condotte dal collettivo Anonymous Italia, sotto la cui egida operano, con sempre crescente autonomia, singole *crew* (AnonPlus ITA, AntiSec ITA e Lulzsec ITA)». La *relazione sulla politica dell'informazione per la sicurezza* viene presentata al Parlamento ogni anno, entro il mese di febbraio, mostrando i dati relativi all'anno precedente. L'*intelligence* nazionale opera a tutela degli interessi economici, politici, militari, scientifici e industriali della Nazione chiamata, costantemente, a misurarsi con sfide globali che implicano la ridefinizione della nozione stessa di sicurezza. Attualmente, la tutela del sistema nazionale, nei suoi plurimi aspetti, si inserisce in un panorama marcato da un'incertezza – non solo economica – alimentata dagli avvenimenti socio-politici degli ultimi tempi, si pensi all'andamento dell'emergenza sanitaria, alle tensioni nell'approvvigionamento di alcuni prodotti e materie prime, e le relative conseguenze.

[28] *Relazione sulla politica dell'informazione per la sicurezza 2020*, p. 9. Anche nel corso del 2021, le azioni ostili in rete – indirizzate verso gli assetti informatici rilevanti per la sicurezza pubblica – hanno continuato ad interessare prevalentemente le infrastrutture informatiche della Pubblica Amministrazione (anche se in diminuzione rispetto al 2020).

celerare quel percorso di riforme verso un approccio normativo idoneo a ponderare responsabilità giuridiche e morali da un lato, diritti e doveri dall'altro.

La relazione propone una dettagliata panoramica degli incidenti virtuali più rilevanti – avvenuti a livello generale –, da cui si apprende che il numero di «attacchi gravi di dominio pubblico», registrati nel primo semestre del 2020, è aumentato del 6,7% rispetto al primo semestre del 2019 (796 contro 850)[29].

Una crescita drastica se si considera che rispetto al 2017 l'incremento è stato del + 37,7%. Il campione di analisi, a giugno 2020, si componeva di 10938 attacchi gravi.

La complessità di questi attacchi è legata all'impatto sulle vittime, in termini di perdite economiche, danni alla reputazione, diffusione di dati sensibili.

Lo studio evidenzia che nel 2019 le categorie *cybercrime*, *cyber*spionaggio e *information warfare* hanno registrato il numero di aggressioni più elevato degli ultimi 9 anni e mezzo: una tendenza confermata anche nel primo semestre 2020[30].

È bene tener presente che attacchi ostili lanciati tra il 2019-2020 non seguono le stesse logiche impiegate nel 2014, e neppure nel 2017, anche se si continua ad utilizzare la stessa denominazione.

L'*Associazione italiana per la sicurezza informatica* afferma che lo scenario emerso da questi dati rappresenta solo *la punta dell'iceberg*, poiché, come spiegano gli esperti, le indagini si riferi-

---

[29] L'aggiornamento di ottobre propone l'analisi degli attacchi più significativi avvenuti, a livello globale, nell'anno precedente e nei primi 6 mesi del 2020. In generale, nel 2021 si è registrato un calo delle attività di matrice *hacktivista*, a dispetto dell'aumento delle azioni a matrice statuale. Queste ultime trovano terreno fertile innanzi ad una generale instabilità politica dovuta sia alle precarie condizioni sociali scaturite dall'instabilità politica internazionale e agli effetti della crisi sanitaria che hanno inciso, quali fattori principali, anche sull'andamento dei flussi dell'immigrazione irregolare verso l'Italia.

In questa dimensione, le risultanze dell'intelligence confermano il radicarsi di operazioni di contrasto che tentano di individuare e neutralizzare le azioni di quei gruppi criminali finalizzate sia alla spartizione di business illeciti, sia all'attenuazione di eventuali spinte conflittuali suscettibili di attirare l'attenzione delle analisi investigative.

[30] *Rapporto Clusit 2020*.

scono ad attacchi reali, effettivamente andati a segno, che hanno provocato danni importanti. Restano esclusi dall'analisi, invece, gli attacchi tentati o bloccati.

Anche il *Cyber Attack Trends: 2020 Mid-Year* rivela che le aggressioni sono aumentate da meno di 5.000 a settimana – nel febbraio 2020 – ad oltre 200.000, verso la fine di aprile. Peraltro, tra maggio e giugno, nei paesi in cui il *lockdown* è stato allentato, gli attacchi virali, non legati all'emergenza Covid, sono aumentati in modo esponenziale.

In generale, lo studio svela che la posizione di attacco non è più occupata da comuni *hackers* ma da gruppi criminali transnazionali che fatturano miliardi, oppure da «multinazionali […] dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence» [31].

Si tratta di organizzazioni belligeranti messe in campo con l'obiettivo di colpire – 365 giorni all'anno e 24 ore al giorno – infrastrutture, reti, *server*, *client*, oggetti *IoT*, fino ad arrivare alla vita interiore delle persone. Il numero di attacchi è in crescita, per questo è urgente individuare e sviluppare sempre nuove strategie difensive.

Si assiste, attualmente, alla nascita di una nuova epoca, di un *altro mondo* del quale non conosciamo ancora la geografia, le regole, le minacce, etc. Emerge, così, una situazione di eccezionale complessità che chiede di discutere e *ri*definire i presupposti giuridici, tecnici ed etici sui quali si dovrebbe basare il corretto funzionamento del *web* e dei servizi che su di esso fanno affidamento, al fine di garantire, anche nel *cyber*spazio, il rispetto della *dignità*: principio primo di ogni vivere sociale [32].

2. *Anonimato, responsabilità e giustizia in rete*

Nei primi mesi del 2020, solo in Italia, si registra un attacco informatico ogni undici secondi; un'intrusione grave ogni cinque

[31] Cfr. *Rapporto Censis 2020.*

[32] L. AVITABILE, *Legalità e giustizia. I Feuerbach e Radbruch*, cit., p. 32 ss.; ID., *Modernità e pensiero giuridico. Persona sistema testo*, Torino, 2013.

ore[33]. Questi dati rappresentano una forte sollecitazione ad osservare la quotidianità digitale che lascia cadere l'illusione di poter associare i *cyber* attacchi ad episodi atipici ed estranei all'esistenza umana[34].

Si rende manifesta, così, l'esigenza di affrontare il problema della *in*sicurezza in rete, percorrendo le traiettorie della giuridicità e della cibernetica, a partire da un'analisi iniziale sugli *scopi* delle minacce informatiche che, in alcuni casi, si presentano nel bivio differenziante di atto intimidatorio e lecita forma di dissenso.

In più occasioni, infatti, alcuni *cyber*-attacchi si sono rivelati come 'pacifici' atti di trasgressione, al pari di una libera manifestazione di volontà, una sorta di raduno popolare in rete.

Nei rettorati di alcune università estere, ad esempio, attraverso l'impiego di DDOS, sono state organizzate manifestazioni di protesta virtuali contro i tagli di bilancio ai fondi per la ricerca e l'istruzione[35].

In questa trattazione, non si intende trascurare la finalità lecita di un *cyber*attacco, quale libera forma di protesta: non se ne riconosce, a prescindere, né la sua illiceità, né la liceità.

Tuttavia, non si possono evitare riflessioni sugli *scopi* delle intrusioni: il tema è complesso ma non esonera dal considerare alcuni problemi. Il silenzio lascerebbe cadere nell'ombra l'insieme delle questioni giuridiche che interessano la responsabilità-imputabilità nei territori inesplorati della rete.

Si è, così, sollecitati ad approfondire le azioni compiute dagli *hackers* che, seppur nascoste nell'anonimia di righe di codice, restano pur sempre condotte orientate alla scelta consapevole di alcuni atti piuttosto che di altri.

Un tentativo per avvicinare la questione dell'anonimato dal

---

[33] *Il* 36% delle compagnie attaccate ha scelto di pagare il riscatto, ma fra queste il 17%, circa una su cinque, non ha recuperato i dati (analisi dei dati di Oren Elimelech).

[34] Cfr. AA.VV., *Cybersecurity Law*, Pisa, 2020.

[35] Nel 2001 una serie di attacchi DDOS colpisce il sito della Lufthansa. Si tratta di una forma di protesta contro la decisione governativa di deportare, con aerei Lufthansa, i richiedenti asilo politico. In quella occasione, la Corte d'Appello tedesca equipara la *cyber*-intrusione ad un *sit-in* virtuale.

punto di vista dell'imputabilità è quello di considerare che «gli atti delle persone – come afferma Romano – sorgono da scelte, pensate e volute, che hanno una motivazione espressa mediante un peculiare linguaggio, quello comunicativo dell'interiorità dell'io, della sua libera personalità»[36]. Le condotte umane sono dirette a rispettare o violare il riconoscimento di ogni individuo, giuridicamente imputabile: ogni persona, nel relazionarsi all'altro, vi si riconosce custodendo la sua originalità esistenziale[37].

Tutto ciò che nella storia concerne la responsabilità/imputabilità del singolo riguarda il momento formativo del questionare sul senso dell'agire[38]. Un soggetto è imputabile quando pensa, forma e realizza una sua intenzione.

Sul *web* si assiste alla formazione di un mondo che non sempre è il risultato di scelte consapevoli, ma è l'esito di un'elaborazione di dati, generativo di un profilo da accettare, inscrivere e concretizzare in una società caratterizzata da una *permissività illimitata*[39].

Nessuno sarebbe imputabile se non fosse responsabile della sua scelta, vale a dire per aver selezionato una determinata azione che concretizza una sua pulsione. Senza una scelta, senza un consenso o un dissenso si è incolpevoli, o meglio, scrive Romano, si è «anonimamente innocenti, come è proprio degli enti del non-umano, dei vegetali, degli animali, delle macchine, anche di quelle cosiddette intelligenti, tutte entità giuridicamente irrilevanti»[40].

Il soggetto esce dalla condizione di innocenza, propria degli animali e delle macchine, avulsa dal fenomeno giuridico, nel momento in cui opera una scelta, e dunque, quando prende una posizione.

Queste analisi riconducono al principio cardine della convivenza umana: *alterum non laedere.* Il principio di Ulpiano invita a considerare la giuridicità come garanzia a non subire lesioni.

---

[36] B. ROMANO, *Algoritmi al potere. Calcolo giudizio pensiero*, cit., p. 9.

[37] ID., *Ingiustizia radicale e narcisismo*, cit., p. 18.

[38] *Ivi*, cit., p. 60. Cfr. G. PETROCCO, *Diritto e sistema dromocratico*, Roma, 2017; B. LEUCADITO, *Diritto digitale, cura dell'esserci e trattamento del dato*, in questo volume.

[39] B. STIEGLER, *L'immunità della filosofia*, Roma, 2021, p. 25.

[40] B. ROMANO, *Ingiustizia radicale e narcisismo*, cit., p. 61.

Il concetto di *offesa* rinvia ad atti, scelte, azioni che non riconoscono l'altro come persona, titolare di diritti incondizionati ed universali, costitutivi della dignità umana.

Una delle maggiori preoccupazioni che accompagnano l'*anomia* della rete attiene proprio alla scarsa consapevolezza dei naviganti sull'utilizzo, da parte di terzi, dei loro dati.

A questo punto sorgono domande. Esiste un *limite* alla pervasività delle azioni ostili in rete? La predisposizione di tecniche di *cyberdefense* – attraverso le quali favorire la riduzione di possibili attacchi – garantisce il rispetto degli *a-priori* del diritto?

Da diversi anni, ormai, il tentativo di limitare, con una regolamentazione *ad hoc*, la condivisione illecita di contenuti malevoli, fallisce. L'anonimato delle transazioni sembra voler proteggere quegli attaccanti che operano, indisturbatamente, per tracciare e controllare milioni di utenti.

La diffusione del crimine cibernetico fa sorgere un duplice ordine di problemi: l'uno di natura psicologica e sociologica; l'altro più propriamente giuridico.

Da qui si avviano alcune considerazioni sulla trasformazione del manifestarsi del diritto nella *civiltà cibernetica* che, inevitabilmente, investe la questione relativa allo *stare in giudizio:* nel dover render conto e dare ragione di una certa azione, fino ad *esplicitare la condizione dell'esser responsabili*[41].

L'aggettivo *responsabilis* descrive colui che**,** per il compimento di determinati atteggiamenti può o deve darne ragione, a causa delle conseguenze che ne sono derivate e che, in qualche modo, hanno invaso la sfera dell'altro[42].

In sostanza, si ritiene giuridicamente responsabile chi deve *rispondere* di un fatto proprio o altrui da cui derivi la violazione dolosa o colposa di un obbligo giuridico, a cui segue, a sua volta, un ulteriore dovere di riparare il danno o ripristinare la condizione originaria.

Una riflessione sull'*imputabilità*, quale fenomeno articolato e multiforme, esige di riprendere il concetto di *colpevolezza* ripercorrendo le tracce della significazione autentica del termine *re-*

---

[41] AA.VV., *Responsabilità, rischio, diritto e postmoderno*, Torino, 2008, p. 21 ss.

[42] *Ivi*, p. 22.

sponsabilità, solitamente accompagnato da attributi che lo definiscono e caratterizzano [43].

Nel diritto civile, l'uso classico della nozione di *responsabilità* è collegato all'obbligo di riparare il danno derivato da un atto illecito colposo, in base a quanto stabilito dalla legge. La responsabilità penale, invece, rinvia all'obbligo di subire una pena [44].

In un momento storico in cui si ritiene che i fenomeni di *cybercrime* possano soggiogare gli esseri umani, si osserva che l'intenzionalità di chi agisce in rete è sottratta ad ogni forma di controllo, punizione e riparazione dei danni causati.

Le tecnologie, nella loro incapacità di *ius dicere* sulla base di motivazioni che hanno generato condotte imputabili, mostrano però una forza oggettivante in grado di processare informazioni e dati personali, consentendo a pochi eletti di introdursi, senza alcun limite, nella vita dei naviganti.

Soprattutto in ambito giuridico, il concetto di responsabilità risente l'incidenza delle nozioni di *danno* e *colpa* [45].

Nella successione di questa trattazione, il binomio imputabilità/responsabilità diventa l'asse portante di un dibattito più ampio che, attraverso la riflessione di P. Ricœur, consente di avvicinare la questione legata alla capacità umana di *diventare* colpevole e, al contempo, di *rischiare* la propria colpa [46].

Il nucleo delle espressioni essenziali su imputazione/imputabilità muove proprio dall'articolato plesso colpa/colpevolezza, che consente di giungere alla constatazione secondo cui «colpevolezza non è sinonimo di colpa» [47].

Sono varie le ragioni che conducono a rifiutare l'idea che esiste una coincidenza tra colpa e colpevolezza. Occorre considerare, in quest'orizzonte, che alla base del concetto di *imputazione* vi è la *capacità di agire* che assume la duplice accezione di imputazioni morale e giuridica.

---

[43] *Ivi*, pp. 25-26.

[44] *Ivi*, pp. 23-24.

[45] AA.VV., *Responsabilità, rischio, diritto e postmoderno*, cit., pp. 144-145.

[46] P. RICOUER, *Finitudine e colpa*, Brescia, 2021, pp. 353-354.

[47] *Ivi*, p. 353.

Considerata da sola, la colpevolezza si dirama in più direzioni, aprendosi ad una riflessione etico-giuridica che interessa il rapporto tra penalità e responsabilità, e non solo. Dall'altro, nel suo significato astratto di *commettere ingiustizia*, ἀδικέω rinvia ad una accezione puramente morale del male, lasciando cogliere che giustizia e ingiustizia affondano le loro radici nella coscienza *del puro* e *dell'impuro*[48].

L'oggetto delle meditazioni qui brevemente riprese riguarda il concetto astratto di responsabilità: dell'essere responsabili di un fatto non solo da un punto di vista giuridico ma anche morale.

Nella visione ricœuriana, alla *responsabilità morale* – in base alla quale si è responsabili di ciò che si è compiuto – subentra la concezione di una *responsabilità prospettica* secondo cui la prevenzione degli effetti dannosi futuri viene ad aggiungersi a quella di riparazione dei danni commessi[49].

Come già accennato, gli eventi determinati dal progresso tecnologico appaiono difficilmente conciliabili con l'idea tradizionale di responsabilità poiché non sono attribuibili ad un soggetto, ad un luogo e ad un tempo.

Comunemente, il soggetto di diritto si ritiene responsabile dei suoi atti – compiuti in un dato momento e in un certo posto – e delle conseguenze da questi prodotte, sia sul versante del diritto [civile e penale], sia su quello generale del bene e del male.

Allora, ci si chiede: che ne è delle azioni ostili compiute nella vastità della rete? L'elemento soggettivo intenzionale [la colpa] può addebitarsi all'autore di un attacco informatico, indipendentemente dalla rivendicazione di un indennizzo?

Attualmente si affacciano in rete nuove generazioni di rischi, derivanti da fenomeni complessi che superano le limitate competenze di controllo e prevenzione delle istituzioni pubbliche, nazionali e sovranazionali.

La convinzione – sempre contestabile – è che, nello spazio cibernetico, si va affermando l'idea di una *colpa senza responsabilità*, retta da un'*anonimia programmatica* che non consente di indi-

---

[48] *Ivi*, p. 353; M. BUBER, *Colpa e sensi di colpa*, cit., *passim*.

[49] AA.VV., *Responsabilità, rischio, diritto e postmoderno*, cit., p. 27 ss.

viduare l'autore di un'intrusione o di una minaccia, determinando inevitabili ipotesi di *de*responsabilizzazione.

Il rinvio a Ricœur appare essenziale per comprendere le profonde ed irreversibili trasformazioni avvicendatesi nel tempo sul concetto di responsabilità [giuridica e morale], a partire proprio dal concetto classico di responsabilità giuridica, che trova nel concetto di imputazione la sua accezione primordiale[50]. Queste brevi considerazioni non hanno alcuna pretesa di valere in modo esaustivo, ma tracciano in modo sintomatico un percorso di ricerca ancora *in itinere*.

3. *Verso una meccanizzazione del diritto*

Definita da Norbert Wiener come l'arte del timoniere, la cibernetica assume i tratti di una scienza che diventa comprensione delle informazioni, e in particolare, dei messaggi di comando[51].

Ricordato per l'attenzione allo studio della tecnica delle comunicazioni e degli strumenti che, nel tempo, hanno dimostrato una sorprendente capacità di imitazione del comportamento umano, le riflessioni wieneriane gettano luce sulla natura delle azioni macchiniche, rivelandone l'attitudine a sostituire quelle umane, scorgendone in maniera quasi profetica, l'inarrestabile progresso.

Attualmente, si viene sollecitati a considerare la peculiare qualificazione del potere delle informazioni e la sempre più incessante produzione di dati, che mostra il rischio di una sproporzione tra chi ha il potere di definire e gestire i messaggi – programmandoli – e chi li esegue – risultandone il destinatario –.

I primi tentativi di costruire sistemi automatizzati sono basati, funzionalmente, su congegni a orologeria. Non a caso, per i suoi approfondimenti sulla struttura dei sensori di ricezione dei messaggi esterni, Wiener si sofferma ad osservare proprio questo antico e sofisticato meccanismo tecnologico[52].

---

[50] Nel suo significato originale di *mettere in conto*, l'atto di 'imputare' implica di ascrivere un fatto a qualcuno. *Ivi*, p. 147.

[51] Cfr. N. WIENER, *La cibernetica*, Milano, 1953.

[52] ID., *Introduzione alla cibernetica. L'uso umano degli esseri umani*, cit., p. 26.

Successivamente, lo studio comparativo tra comportamenti umani e sistemi macchinici lo porta ad analizzare il movimento delle figurine sulla sommità di un *carillon*: seguendo un modello specifico, in base al quale i movimenti passati non influenzano in alcun modo quelli successi, le figurine si spostano eseguendo un messaggio univoco che parte dal *carillon*, arriva alle statuette e lì si esaurisce.

Si coglie che questi *output* non promanano da una condizione *naturale*, ma derivano da un processo di elaborazione che trasforma le informazioni in comandi da eseguire.

Wiener osserva che, in tali casi, non vi è traccia di una interazione con il mondo esterno e, nella loro condizione di sordità, cecità e mutismo le figurine non possono modificare la loro condizione: non possono discostarsi dallo schema predisposto nel modello convenzionale del *carillon*.

In generale, ogni comportamento automatizzato è determinato dall'immissione di dati, tramite schede perforate o nastri, che stabiliscono, in modo univoco, come la macchina deve agire in una data situazione.

Gli esseri umani, invece, affermano se stessi attraverso il dialogo, nella capacità di rischiare la propria libertà, attraverso condotte giuridicamente imputabili, mai predeterminate e determinabili.

Muovendo dal confronto tra l'operosità prevedibile della macchina e la spontaneità delle condotte umane si giunge alla distinzione tra automi e sistemi giuridici. «È mia convinzione – scrive Wiener – che il comportamento degli individui viventi è esattamente parallelo al comportamento delle più recenti macchine per le comunicazioni; […] in entrambi – spiega – esiste un apparato speciale per raccogliere informazioni dal mondo esterno […], e render[le] utilizzabili nel comportamento dell'individuo o della macchina»[53].

Il funzionamento del *carillon* non rappresenta il modello specifico di tutti i comportamenti automatici ma, come in ogni macchina, il suo funzionamento si contrappone a quello degli esseri umani.

Le considerazioni che seguono sono dedicate alla problematizzazione di tali questioni, nell'ottica di approfondire il modo in cui le tecnologie diventano un duplicato dell'umano.

---

[53] *Ivi*, p. 29.