IL BENE GIURIDICO DELLA SICUREZZA DELLE RETI ALLA PROVA DELLA GAMES THEORY. IL PROBLEMA DELL'HACKING ETICO *

Claudio de Giacomo**

SOMMARIO: -1. Premessa. - 2. L'analisi della sicurezza dal punto di vista della Teoria dei Giochi. -3. Modelli di gioco e sicurezza delle reti. - 4. L'hacking etico e il problema giuridico della sicurezza delle reti.

1- Premessa.

La crescente domanda di norme dirette a regolare i diversi aspetti del mondo delle nuove tecnologie, in particolare di quelle che incrociano l'intelligenza artificiale con il web, ha fatto crescere, anche dal punto di vista dell'informatica giuridica, la riflessione sui modelli teorici in grado di rappresentare più efficacemente la complessità dinamica dei fenomeni criminali legati a tali realtà in rapida evoluzione.

Si pensi in generale al numero, al grado e alla qualità delle sanzioni, anche penali, introdotte dal GDPR (UE) 2016/679, il Regolamento generale sulla protezione dei dati, rispetto alla previgente disciplina nazionale in tema di protezione dei dati; e si consideri, poi, in particolare, quanto sia divenuta attuale la verifica della funzionalità dei sistemi di protezione dal punto di vista degli adempimenti, a seguito dell'introduzione nell'ordinamento italiano della previsione di ispezioni disposte dal Garante per il trattamento dei dati personali.

Le ispezioni privacy, si realizzano con l'accesso e le verifiche su tutte le banche dati e gli archivi dove si svolga il trattamento di dati personali ed hanno luogo con la collaborazione delle Forze dell'ordine e di esperti informatici, per lo più senza preavviso, tant'è che per esse si utilizza un termine già in voga per le ispezioni fiscali, quella di *dawn raid*.

Il moltiplicarsi negli ultimi anni del volume di accessi abusivi ai sistemi di proprietà di privati o di Enti pubblici, ha reso allarmante l'esigenza di proteggersi dagli attacchi che provengono dalla rete; fenomeno reso più urgente dal contemporaneo aumento delle utenze mobili, del volume delle banche dati (sopratutto di quelle pubbliche che gestiscono ingenti quantità di dati sensibili) e dell'utilizzo di applicazioni digitali sulla rete.

In tal senso risulta centrale, anche per le conseguenze giuridiche che possano derivarne, sia la DPIA, ovvero la valutazione d'impatto sulla protezione dei dati, che il ruolo via via crescente del DPO, il responsabile della protezione dei dati.

Si tenga conto, in via esemplificativa, di quanto il crescente utilizzo delle tecnologie *wireless* abbia reso progressivamente vulnerabili le reti alle possibili intrusioni degli *hacker* e di quanto le tecniche sempre più sofisticate degli attacchi abbia in tempi recenti indebolito tradizionali misure di sicurezza rappresentate dai *firewall*.

Un potenziale intrusore, nella maggior parte dei casi, non penetrerà nel sistema attraverso il *firewall,* ma individuando il punto meno sicuro del sistema, l'anello debole della catena. E' stato stabilito, infatti, che oltre l'80% degli attacchi alle reti informatiche è

* Testo rivisto della lezione tenuta al corso di dottorato di ricerca in Scienze Giuridiche a.a. 2018-2019.

** Professore aggregato di Logica Giuridica- Dipartimento di Scienze Giuridiche dell'Università di Salerno

da attribuirsi a banali errori umani, come possono essere quelli di un dipendente che collega la personale chiave USB alla postazione di lavoro, l'apertura di mail contenenti *virus*, la ripetizione di *password* non sufficientemente complesse sugli *account* aziendali ecc.[1] Il risultato di tali pratiche può compromettere la sicurezza del sistema nel suo complesso, ed è per questo che le ispezioni privacy hanno uno svolgimento tutt'altro che formale, come può essere quello basato sulla semplice acquisizione di formulari cartacei che spesso rispondono alle consuete logiche ripetitive del genere copia-incolla, ma sono invece dirette ad accertare in concreto l'affidabilità delle misure adottate dagli amministratori del sistema per la protezione degli stessi e delle reazioni in caso per esempio di *databreach*.

Ora, per quanto multiforme si presenti la fenomenologia di queste nuove realtà criminali, che sono in costante e rapida evoluzione, il quadro di riferimento naturale dei problemi della sicurezza dei sistemi, può essere ricondotto al modello teorico-base per la risoluzione dei conflitti, che è a sua volta basato su una classica dinamica di interazione strategica della teoria dei giochi a due parti, quella di chi attacca e quella di chi si difende.

Gli obiettivi dei giocatori, in tale contesto, si presentano obiettivamente confliggenti, per quanto varia possa essere la loro fenomenologia. Per esempio, a fronte di una ricerca di soluzioni, da parte degli amministratori, che garantiscano sempre una certa funzionalità del sistema pur se a livelli diversi, che è l'obiettivo naturale di chi si difende dagli attacchi, dall'altra parte gli obiettivi possono diversificarsi: da quello puramente demolitorio, diretto a distruggere il sistema ovvero a danneggiarlo in modo più o meno radicale, a quelli variamente indirizzati a menomare le difese del sistema per ottenere dei vantaggi, dando l'impressione che esso continui a funzionare regolarmente, mentre in realtà alcune parti sono manovrate in remoto per il raggiungimento degli scopi particolari di chi ha realizzato l'attacco.

2- L'analisi della sicurezza dal punto di vista della Teoria dei Giochi

L'analisi di dinamiche conflittuali di questo tipo, con i relativi incroci di comportamenti strategici, rappresenta lo scenario naturale della Teoria dei giochi.

Di solito le rappresentazioni di queste dinamiche non possono essere analizzate in termini deterministici, esse si presentano piuttosto come giochi stocastici con un alto numero di variabili da considerare, un largo impiego di logiche probabilistiche e di strumenti inferenziali per analizzare da un lato le prestazioni dei sistemi e dall'altro per rendere prevedibile, entro un certo grado almeno, le possibili varianti di attacchi ai sistemi stessi. Tutto ciò evidentemente allo scopo di approfondire il *payout* associato alle possibili decisioni di entrambe le parti del gioco, con al centro l'obiettivo della vulnerabilità del sistema.

Da tali punti di vista la Teoria dei giochi rappresenta l'approccio metodologico più adeguato a considerare l'ambiente decisionale di situazione strategiche interattive in cui le parti avendo obiettivi oggettivamente in conflitto hanno la necessità di considerare i possibili ambiti decisionali del proprio avversario prima di decidere le proprie mosse.

[1] Si pensi a casi anche recenti in cui gli intrusori riescono ad appropriarsi di credenziali di autenticazione ai sistemi delle PP.AA. introducendosi in banche dati come quelli dell'Agenzia delle Entrate, dell'Inps, di Infocamere, ecc. per esfiltrare le informazioni personali di cittadini ed imprese o per condurre operazioni di profilatura delle stesse, per poi "rivenderle", nel migliore dei casi, sotto forma di servizi abusivi in favore degli interessati. La tecnica di *phishing* utilizzata consiste spesso in semplici messaggi di posta elettronica che provengono apparentemente da Enti Pubblici, inducendo gli operatori a cliccare su un banale allegato che in realtà apre la porta a sofisticati virus informatici per mezzo dei quali gli *hacker* assumono il controllo della rete dei computer infetti, in qualche caso utilizzando potenze di calcolo moltiplicate da potenti *Botnet*, controllate in remoto da centrali installate su server posizionati all'estero.

Approfondimenti di questo tipo si rendono necessari non solo per le parti in gioco, ma innanzitutto per chi è chiamato a dettare, in un certo senso almeno, le regole del gioco stesso, ed è per tale ragione che in apertura di questo lavoro si faceva riferimento al crescente bisogno di norme che regolino lo spazio di cui parliamo. Una tale esigenza, a parere di chi scrive, non può essere soddisfatta senza una adeguata conoscenza dei modelli teorici di base che presiedono alle dinamiche di interazione strategica cui si accennava.

La Teoria dei Giochi è una disciplina che nasce in ambito economico, e la sua data di nascita coincide con la pubblicazione nel 1944 del celeberrimo "*Theory of Games and Economic Behavior"* di John von Neumann e Oskar Morgestern [2]. Con questo lavoro i due studiosi gettarono le basi di una teoria generale delle situazioni di interazione strategica, cioè di quelle situazioni della vita comune nelle quali la decisione è riconducibile non ad un decisore unico ma all'interazione di più soggetti in competizione tra loro. La grande intuizione alla base di questo straordinario programma di ricerca fu di individuare nella descrizione dei diversi tipi di giochi, nonché degli atti e delle strategie a disposizione dei giocatori, il modello generale per la comprensione dei comportamenti razionali in tutti i casi in cui l'esito di una decisione dipende in qualche misura da più persone e cioè dai partecipanti al gioco stesso, e più precisamente ancora dipende dalle scelte che essi realizzano nel corso del gioco. Ma fondamentale lungo questo percorso è stato il contributo di uno dei massimi teorici della Teoria dei Giochi applicata alle scienze sociali, Thomas Schelling, e segnatamente l'analisi innovativa, collocata negli anni 60 dello scorso secolo, degli strumenti applicabili alle procedure di negoziazione, da quelle internazionali a quelle contrattuali: si pensi all'efficacia di meccanismi essenziali come quelli fondati sul binomio minaccia-promessa, basati in definitiva sul grado di credibilità di chi si avvale di tali strumenti, ovvero sulla capacità di provare la convenienza ex post a portarle effettivamente a compimento.[3]

Le applicazioni della TG nel corso degli anni sono cresciute di pari passo alla comprensione della trasversalità dei metodi e della versatilità dell'impianto logico-matematico che assiste tale teoria. Così, dall'originario ambito economico, la *Games Theory* si è allargata a settori un tempo impensabili diventando il paradigma dell'analisi della scelta razionale in contesti diversi, dai mercati finanziari alla politica, dai negoziati internazionali alla comprensione dei meccanismi di interazione biologica tra specie animali, dalle scelte sugli impieghi delle risorse pubbliche all'etica e in generale al ragionamento pratico ivi incluso quello dedito all'analisi di fenomeni criminali.[4]

A tal riguardo va sottolineato come la Teoria dei Giochi abbia interessato, sopratutto nei Paesi di *Common Law*, le analisi sui meccanismi di funzionamento dei sistemi giuridici che rappresentano, per tanti versi, un terreno di elezione naturale di metodologie riferite alla scelta razionale.[5]

Lo scenario particolare che prendiamo in considerazione per il caso di specie è quello dei cosidetti giochi stocastici, ovvero, quel tipo di giochi nel quale le parti interagiscono tra loro in termini strategici, dovendo prendere delle decisioni in base alle

[2] id., *The Theory of Games and Economic Behavior*, 3rd ed Princeton N.J., Princeton University Press, 1953

[3] T. Shelling, *The Strategy of Conflict,* Harvard University Press, Cambridge Mass., 1960; tr. it *La strategia del conflitto,* Milano, Mondadori B., 2006.

[4] Si consideri in tal senso un classico come G.S.Becker, "Crime and Punishment: An Economic Approach." in *Journal of Political Economy* 76.2 -1968. Gary Becker (che riceverà per i suoi studi il premio Nobel nel 1972), per la prima volta in questo testo offriva un'analisi rigorosa del crimine dal punto di vista della razionalità della teoria dei giochi; a tale approccio si sono ispirati nei decenni successivi numerosi filoni di studio che hanno preso come punto di riferimento i metodi della scuola di Chicago.

5 Uno dei primi contributi a carattere generale sull'argomento è stato D. Baird, R. Gertner, R. Picker, *Game Theory and Law*, Cambridge, MA: Harvard University Press, 1994.

limitate informazioni che possiedono, sopratutto quelle del più recente passato, cercando in tal modo di trovare la migliore condotta di gioco per il momento attuale e per l'immediato futuro; naturalmente, le possibili mosse in contesti di questo genere variano in range di tipo essenzialmente statistico-probabilistico.

I giocatori, intesi qui come gli amministratori del sistema, da una parte, e gli aggressori professionali, dall'altra, non è detto che debbano vincere o perdere, teoricamente potrebbero continuare a giocare una partita infinita.

La situazione che abbiamo davanti è il classico scenario delle decisioni interdipendenti, e la teoria dei giochi secondo una delle definizioni di Schelling è « *lo studio di come individui razionali prendano decisioni quando la scelta migliore tra due scelte possibili, o quella tra le diverse possibili, dipende dalle scelte che gli altri compiranno o stanno compiendo.* » [6]

Ciò che costituisce lo specifico della situazione in esame è il fatto di trovarsi in presenza di un particolare tipo di gioco che si definisce stocastico. Vale a dire una situazione nella quale i giocatori si trovano a dover seguire le regole, tutte o almeno una parte di esse, con modalità di tipo statistico.

Ci si metta dal punto di vista dell'amministratore di una rete o di una banca dati, partendo dalla considerazione dei costi progressivi della sicurezza e del limitato numero di risorse economiche a disposizione per difendersi da potenziali attacchi, nonchè dalla consapevolezza che nessun sistema difensivo può considerarsi una cittadella del tutto inespugnabile. A questo punto, la razionalità delle scelte strategiche da porre in campo può essere, in certo qual modo, misurata sulla base dei modelli di interazione tra potenziali intrusori e sistemi di rilevamento delle intrusioni, con l'impiego di un certo numero di risorse, basandosi su regole di transizione di tipo probabilistico.

Nel quadro così sommariamente delineato, prendono posto una quantità di variabili che tengono conto, entro certi limiti, della variabilità degli attacchi, della loro distribuzione sulla rete , e delle possibili reazioni in difesa del sistema. [7]

Gli elementi di base del gioco, dal punto di vista della sicurezza della rete, non sono diversi da quelli che la *Games Theory* individua come tipici di ogni interazione strategica.

La Teoria dei giochi, infatti, si applica ai problemi di decisione razionale in tutti i casi in cui il risultato finale dipende dall'interazione delle scelte di due o più persone.

Gi elementi che non possono mai mancare in un gioco vengono individuati di solito nei seguenti.

1) La pluralità di soggetti partecipanti. Non necessariamente deve trattarsi di due persone, può trattarsi di soggetti complessi come due partiti o due nazioni, oppure, come nel nostro caso, di due categorie ben distinte che rinviano a realtà più ampie di quelle individuali, aziende, Enti, gruppi terroristici ecc., ovvero quelli che attaccano per danneggiare un sistema e quelli che sono interessati a difenderlo. Ciò che rileva dal punto

[6] T. Shelling, *Micromotives and Macrobehavior* ,2006 W.W. Norton &Company inc., tr. it. *Micromotivazioni della vita quotidiana*, Milano, Bompiani, 2008, p. 10.

[7] La letteratura specialistica su tali argomenti è molto vasta e va ampliandosi in maniera esponenziale. Tra i moltissimi riferimenti al riguardo si rinvia a Han, D.Niyato, W.Saad, T.Baar, A.Hjorungnes *Game Theory in Wirelessand Communication Networks: Theory, Models, and Applications*,Cambridge University Press, 2011; K.W. Lye and J. Wing, *Game strategies in network security*, Foundations of Computer Security Workshop in FLoC 02, Copenhagen, Denmark, 2002; E.O. Ibidunmoye, B.K. Alese, O.S. Ogundele, "A Game-theoretic Scenario for Modelling the Attacker-Defender Interaction", in *Computer Engineering Information Technology*, 2013; Y. Lin, Y. Wang, Y. Wang, and H. Zhu, "Stochastic Game Nets and Applications in Network Security", in *Journal of Computers*, 2009, pp. 461-467.

di vista del gioco è che la strategia imputabile a ciascuna parte si rappresenti in maniera unitaria.

2) Un certo numero di strategie a disposizione per ciascuno dei partecipanti, ovvero un insieme di mosse che i giocatori hanno a disposizione nel gioco. Tale possibilità di scelta non può mancare in alcun caso. Del resto anche più in generale, ogni problema di decisione anche di tipo individuale, per potersi definire tale, deve includere una possibilità di scelta, in assenza della quale ci troveremmo piuttosto di fronte ad atti vincolati che sono estranei agli argomenti di cui ci occupiamo.

Consideriamo lo specifico del gioco di cui ci stiamo occupando.

Uno dei metodi di base nella protezione di una rete è rappresentato dai cosidetti *firewall* che vengono utilizzati contro possibili intrusioni dei tipi più diversi, dallo *spam* ai cavalli di Troia, alla varietà di *spyware*.

Il modo più semplice col quale gli intrusori cercano di aggirare i sistemi non protetti è quello di inviare *ping* via Internet, come può essere la composizione casuale di numeri di telefono: il sistema che risponde diventa la vittima potenziale. Da questo punto di vista, qualsiasi elaboratore connesso a una rete esterna è a rischio. Il *firewall* svolge la funzione di uno scudo, esaminando il traffico di rete prima di accedere alla rete stessa e autorizzando i dati trasferiti utilizzando alcune protocolli di sicurezza. Se il pacchetto di dati è incerto, il *firewall* lo bloccherà.

Quante sono in questo caso le scelte di azione a disposizione del difensore? Molteplici: controllare l'ingresso attribuendo diversi *grant* di accesso a persone diverse; implementare la formazione degli utenti per anticipare la soglia di protezione con misure preventive che esaminino continuamente il registro degli accessi, ecc. ma la varietà di strategie a disposizione si amplia di continuo.

3) Un certo insieme di regole che definiscono le mosse consentite nel gioco e quelle che non vi appartengono. Naturalmente bisogna fare bene attenzione a non confondere regolarità delle mosse e strategie di gioco. Altro è conoscere la mossa corretta del pezzo del "cavallo" nel gioco degli scacchi, altro è conoscere quanto sia opportuno muoverlo in una situazione di gioco concreta per dare scacco, per esempio, al re avversario, lasciando scoperta una certa diagonale.

Dal punto di vista del gioco che ci occupa nel presente lavoro, il primo dilemma relativo alle azioni da compiere nel gioco è quello di nodi successivi di alberi decisionali da ambo le parti: per l'attaccante il primo nodo sarà quello relativo alla scelta tra attaccare o non attaccare, e per chi si difende sarà quello alzare il livello di difesa rispetto a quello esistente, se ne esiste già uno in azienda, o non impegnare risorse aggiuntive, fino alla scelta estrema di apprestare difesa zero al sistema.

4) Un insieme di esiti possibili, cioè di *pay-off* associati alle scelte compiute dai giocatori. Nel nostro caso è l'obiettivo finale che rileva dopo che tutti i rami dell'albero decisionale sono stati percorsi e tutte le mosse sono state giocate. A questo punto il *payoff* segnalerà il conteggio di vulnerazioni del sistema, le difficoltà al funzionamento ordinario che tali penetrazioni hanno causato, ovvero i danni procurati per il ripristino della corretta funzionalità di esso, commisurati al costo delle risorse impegnate; costo che rappresentato da una sommatoria di elementi complessi, in quanto la sua misura non è rappresentabile direttamente solo nei termini contabili del capitolo di spesa, ma comprende il numero di addetti alla sicurezza, il tempo impiegato per tale *mission*, la larghezza di banda impegnata e così via. Dall'altra parte, anche per l'intrusore esiste un *payoff* che può misurarsi in termini positivi o negativi, associato al grado di vulnerazioni inflitte al sistema, al numero di esse, al livello di sensibilità dei dati sottratti, alle possibili utilizzazioni di tali dati ed alle eventuali remunerazioni che sia possibile ricavarne, il tutto commisurato al costo dei rischi che si corrono, ed in primo luogo quello di essere individuati e di essere perseguiti per l'accesso

abusivo al sistema e per gli eventuali danni o abusi perpetrati, alla confisca delle attrezzature ecc.

Non va sottovalutata, infatti, la severità nell'ordinamento italiano delle conseguenze dell'intrusione in sistemi informatici e telematici, prevista e punita in primo luogo dall'art. 615 ter C.P., che nei casi aggravati dalla distruzione o dal danneggiamento del sistema o dall'interruzione anche solo parziale del funzionamento o dei dati e programmi in esso contenuti, statuisce la pena della reclusione da uno a cinque anni, e la procedibilità d'ufficio in caso di denuncia.

Dal canto suo, l'obiettivo dell'amministratore sarà evidentemente quello di disporre un'allocazione ottimale delle risorse ritenuto indispensabile dal punto di vista delle risorse a disposizione per proteggere con successo il sistema, mentre l'obiettivo dell'attaccante è penetrare nel sistema per vulnerarlo in qualche modo.

3- Modelli di gioco e sicurezza delle reti.

Oltre agli elementi appena visti dobbiamo considerare le assunzioni per tanti versi implicite che la *Games Theory* associa alla razionalità strategica.

a) In primo luogo si assume che i giocatori siano intelligenti. Questa assunzione è tutt'altro che banale, essa riguarda la capacità dei giocatori di comprendere perfettamente le situazioni nelle quali si trovano e di orientarsi correttamente in ogni momento senza mai commettere errori o distrazioni: detto in altro modo, si presuppone che i giocatori siano sempre in grado di scegliere per il meglio nelle situazioni concrete sulla base delle informazioni a disposizione. Questa assunzione potrà apparire per molti versi restrittiva e quindi poco realista perchè in molti casi gli uomini si comportano in modo diverso: possono essere stanchi o distratti; ovvero, possono decidere per motivi diversi da un calcolo razionale orientato sulle conseguenze, pensiamo alla natura emotiva di tante decisioni che vengono prese nel corso di una comune giornata. Tuttavia, la TG presenta modelli della realtà (come accade per qualsiasi teoria), e per quanto questi possano essere fedeli ci sarà sempre una distanza di qualche tipo dalla realtà che con essi s'intende rappresentare. Nessuna carta geografica contiene la riproduzione esatta di tutte le minime asperità del terreno, ognuna delle quali può essere d'inciampo. Cionondimeno, pur nelle loro imprecisioni, esse ci danno un valido aiuto quando ignoriamo la direzione da prendere.

Allo stesso modo, la TG prende in considerazione un sottoinsieme significativo di decisioni che possiamo definire "razionali"[8], ma dovremmo piuttosto correttamente qualificare "intelligenti", senza che ciò comporti alcun problema nel dover ammettere che spesso le motivazioni che spingono gli uomini a prendere decisioni nelle situazioni concrete siano di ordine diverso da quelle dettate dalla pura razionalità.

b) Un'altra assunzione implicita della Teoria dei giochi è che ogni giocatore persegue i propri interessi con lo scopo primario di massimizzare l'utilità attesa. Può sembrare banale doverlo ricordare ma nessuno gioca per perdere. La Teoria dei giochi non si occupa di altruismo, generosità, solidarietà, nè di altri nobili sentimenti. Così come non si occupa di sentimenti cosidetti infami. Non importa quali siano gli obiettivi o gli atteggiamenti di vita dei giocatori, sappiamo solo che una volta entrati nel gioco, si considererà razionale privilegiare le strategie che massimizzano i benefici e minimizzano i costi. Anche questa assunzione, a ben vedere, costituisce una restrizione rispetto ai comportamenti reali degli

[8] In senso formale la razionalità delle decisioni è un concetto più ristretto di quello considerato nel testo, perchè è associato al principio logico della transitività secondo il quale se *a* è preferito a *b*, e *b* è preferito a *c*, allora *a* è preferito a *c*. In simboli : $a \succ b \wedge b \succ c \rightarrow a \succ c$.

attori sociali che in molte situazioni della vita possono essere spinti ad assumere decisioni sotto la spinta di ideali e stili di vita che rispondono ad esigenze diverse. La Teoria dei giochi non giudica questi stili di vita ma si limita a valutare le scelte sotto il profilo della razionalità strettamente orientata alla massimizzazione dei risultati ottenibili nel gioco.

Queste ultime considerazioni ci danno modo di riferirci ad alcune delle principali classificazioni che la Teoria propone riguardo ai giochi, allo scopo di individuare la peculiare natura dell'interazione strategica di cui ci occupiamo nel presente contributo.

La prima distinzione riguarda la differenza tra giochi a somma-zero e giochi a somma variabile. Nei primi si realizza il massimo della contrapposizione, nel senso che perdite e guadagni si equivalgono annullandosi, e quindi il guadagno di una parte corrisponde ad una perdita di segno contrario dell'altra parte. Nei giochi a somma variabile, invece, tale vincolo non sussiste, come nel caso dei giochi cooperativi, dove è possibile che tutte le parti ottengano insieme un miglior risultato finale o perdite maggiori.

Nel nostro caso siamo in presenza di un classico caso di gioco a somma zero, nel senso che perdite e guadagni si annullano, ovvero il maggior guadagno per una parte corrisponde ad una maggiore perdita dell'altra.

Un'altra importante caratteristica riguarda poi la differenza tra i giochi a informazione completa, come possono essere gli scacchi o la dama, e i giochi a informazione incompleta, come il poker, nei quali cioè ogni giocatore non conosce, prima della fine del gioco, le carte che gli avversari hanno in mano, ciò che determina essenziali varianti nella valutazione di razionalità delle strategie seguite. Nel caso allo studio ci troviamo evidentemente in presenza di un gioco a informazione imperfetta.

L'informazione ha un ruolo centrale nell'analisi del gioco e delle sue dinamiche sopratutto da due punti di vista.

La strategia dei giocatori, cui abbiamo già accennato, che è funzione diretta delle informazioni a loro disposizione ed in base a queste ultime è possibile massimizzare il *pay-out* finale per ambo le parti. Direttamente collegata all'elemento appena visto è l'individuazione del punto di equilibrio del gioco, sul quale realizzare un meccanismo di risposta efficace e credibile. Con riferimento a quest'ultimo va ricordato che un teorema fondamentale della teoria dei giochi, stabilisce che esiste sempre un punto in cui tale equilibrio si realizza, almeno nei giochi a somma costante. [9]

In casi di questo genere non esiste una strategia pura da adottare dall'inizio alla fine del gioco, anzi insistere sulla stessa strategia risulterebbe alla lunga dannoso. Quella che nell'opinione corrente viene spesso presentata come una posizione "forte", nel senso di essere ferma e irremovibile, in molti casi analizzabili dalla teoria dei giochi si rivela essere una posizione "debole", perchè la prevedibilità delle mosse dell'avversario fornisce informazioni di cui l'altra parte può utilmente giovarsi. L'essenza di una strategia mista, invece, consiste nella variabilità delle mosse e quindi nella possibilità di avvantaggiarsi del cosidetto fattore sorpresa.

L'obiettivo di chi analizza un gioco è proprio quello di individuare una soluzione che fornisca ai giocatori i massimi rendimenti con i costi minimi. Se tale punto esiste i giocatori, se razionali, non saranno disponibili a deviare da tale stato perchè porterebbe a rendimenti minori.

[9] La prima formulazione del teorema del *minimax,* dovuta a von Neumann, risale al 1928; essa inizialmente si applicava solo ai giochi a somma zero e ad informazione piena. Successivamente, il teorema fu esteso ai giochi ad informazione parziale e a quelli con più di due giocatori. L'estensione di cui ci occupiamo nel testo è quella con la quale si stabilisce che per ogni gioco a somma zero con due giocatori che hanno a disposizione un insieme finito di strategie pure, vi è sempre almeno un equilibrio di strategie miste. Cfr. von Neumann- O. Morgestern, *The Theory of Games and Economic Behavior,* cit.

Nel nostro caso ci muoviamo in uno spazio caratterizzato da modelli stocastici perchè i giocatori compiono le loro mosse e realizzano le proprie strategie di una struttura informativa parziale, basata per lo più su conoscenze desunte dal passato più o meno recente.

Un gioco stocastico è di tipo dinamico, e si attua attraverso fasi di natura probabilistica. I giocatori sono costretti a selezionare le azioni nel gioco sulla base delle conoscenze necessariamente parziali sull'ambiente. Perchè parliamo di gioco dinamico? Perchè esso di solito evolve in nuove fasi del gioco, in cui i giocatori sono chiamati a sviluppare nuove strategie sulla base delle fasi attacco/difesa precedenti, dando luogo a processi efficacemente rappresentati dal punto di vista statistico dal modello delle catene di Markov.

Lo spazio ridotto di un articolo non consente un'approfondita analisi di questi modelli del gioco se non con riguardo ad un aspetto che riteniamo fondamentale riguardo al problema specifico analizzato nel presente contesto.

Considerando che i giocatori provano a massimizzare le proprie azioni in un contesto competitivo, gli equilibri realizzabili dal punto di vista teorico sono di diverso tipo. Esistono approcci diversi per la soluzione di un gioco e la strategia del minimax, nel senso di Nash, che rappresenta solo una di esse, si pensi in primo luogo all' alternativo equilibrio bayesiano che contiene numerose modifiche al modello di Nash.

Ogni tipo di equilibrio nella teoria dei giochi si struttura, ad ogni modo, attorno alla centralità delle informazioni a disposizione del giocatore.

L'analisi dell'interazione strategica tra amministratore di sistema col suo *staff* tecnico da una parte, e l'*hacker* dall'altra, realizza un peculiare modello considerando la struttura dell'informazione, in grado di restituire lo schema di base delle diverse strategie che i giocatori potrebbero seguire.

Dal punto di vista della Teoria dei Giochi, un gioco in cui ogni giocatore possiede la conoscenza delle azioni di tutti gli altri giocatori che hanno già avuto luogo, è definito un gioco con informazioni complete e perfette. Conoscere le strategie e i rendimenti degli altri giocatori significa avere la conoscenza della storia completa del gioco. Naturalmente, questa è una condizione possibile ma è una condizione-limite per l'interazione strategica, sopratutto nell'ambito del modello che stiamo considerando che ha per tema la sicurezza delle reti, nelle quali i giocatori non avranno di solito una conoscenza deterministica dei ritorni delle loro strategie, anche in forza di una conoscenza parziale dell'ambiente, delle mosse possibili degli altri giocatori come dei loro *pay-off*.

4- L'hacking etico e il problema giuridico della sicurezza delle reti.

La struttura informativa gioca dunque un ruolo centrale nella definizione delle dinamiche associate alla sicurezza dei sistemi informatici.

Da tale punto di vista è interessante notare come nell'ordinamento giuridico sia la stessa latitudine della nozione di attacco o di violazione del sistema ad essere in qualche caso problematizzata e distinta dal significato intuitivo che ad esso si associa nell'art. 615 ter del Codice Penale.

La stessa incertezza semantica delle definizioni legislative, complice forse l'inadeguata comprensione dei fenomeni in evoluzione, sta rendendo più difficili o se si vuole meno scontati gli esiti di condotte che tradizionalmente avremmo associato alla violazione dei sistemi informatici.

Si consideri come, recentemente, si sia aperta qualche crepa attorno all'idea stessa, per tanti versi inadeguata di violazione del sistema, ricavata dall'idea naturalistica della violazione del domicilio informatico.

In base a tale definizione, "chiunque" può essere punito per l'oggettività del fatto di introdursi in un sistema informatico o telematico protetto da misure di sicurezza o di restarvi, "contro la volontà espressa o tacita di chi ha il diritto di escluderlo".

La problematicità delle situazioni in gioco è resa evidente da una recente decisione del GIP del Tribunale di Catania, che è ancora presto per dire se avrà un seguito o sarà destinata a restare una pronuncia isolata. [10]

Nel provvedimento di cui si parla, il Giudice per le indagini preliminari accoglieva la richiesta di archiviazione proposta dal Pubblico Ministero nel procedimento a carico di un soggetto, indagato per aver realizzato un evidente e massivo hackeraggio ai danni di un sistema informatico. Va dato atto che la parte offesa, rappresentata dalla proprietà del sistema violato, si era opposta alla richiesta di archiviazione.

I fatti denunciati dalla società proprietaria di un'applicazione per *smartphone*, riguardavano il caso di un esperto informatico che, senza esservi autorizzato, penetrava a più riprese nel sistema della società proprietaria.

Successivamente alla violazione del sistema, l'hacker indirizzava alla società stessa una serie di mail per circa un mese per denunciare di aver rilevato un certo errore di sistema nell'applicazione, ciò che nel gergo tecnico viene definito un *bug*.

Poichè l'azienda proprietaria del software non rispondeva alle mail, l'intrusore divulgava nel suo *blog* gli errori di sistema riscontrati nell'applicazione rendendo noto quindi, ad una varietà indeterminata di persone, anche l'accesso abusivo per mezzo del quale aveva potuto riscontrare il *bug* di cui trattasi.

Fin qui i fatti nella loro essenzialità. Interessante, però, è la decisione con la quale il G.i.p. del Tribunale di Catania riteneva di archiviare la posizione dell'indagato ritenendo che il fatto non costituisca reato, non avendo integrato il comportamento dell'indagato la fattispecie di accesso abusivo di cui all'art. 615 ter C.P.

Nella motivazione del provvedimento, infatti, il Giudice rileva in premessa che nella gestione dell'attività di impresa la sicurezza dei sistemi informatici ha una crescente rilevanza. D'altra parte costituisce "prassi consolidata" quella dei titolari delle aziende che invitano a comunicare, a chi ne abbia avuto conoscenza, gli errori di sistema rilevati nell'apparato.

Nel caso di specie, il provvedimento di archiviazione si basa sulle missive indirizzate dall'indagato alla Società e sull'inerzia che quest'ultima avrebbe avuto nel correggere le "vulnerabilità del sistema".

Il ragionamento giudiziale che ha condotto a ritenere la mancata ricorrenza del delitto di cui all'art 615 ter, si basa quindi, in definitiva, sulla ritenuta non rimproverabilità del comportamento tenuto dall'indagato che da tale inerzia sarebbe stato indotto a divulgare sulla rete i *bug* rilevati nel sistema.

Tale comportamento, qualificato dal giudice come "divulgazione responsabile", renderebbe non punibile il comportamento, che andrebbe per tale motivo qualificato nei termini del cosidetto "*hacking* etico", espressione utilizzata appunto per riferirsi all'attività di quanti, in possesso di competenze tecniche non comuni, compia attacchi informatici non al fine di danneggiare quanto piuttosto di informare il titolare del sistema sull'esistenza di un problema nella sicurezza.

Alla luce di tali considerazioni, ad apparire "colpevole", è piuttosto la decisione dell'Azienda per non aver apprestato in tempo utile le contro-misure necessarie a risolvere il bug di cui trattasi.

La decisione appare nel suo esito non precisamente scontata sopratutto considerando l'arresto della Suprema Corte di qualche anno precedente, riferito alla nota

[10] Tribunale di Catania, Ufficio del G.i.p., decreto 15 luglio 2019.

vicenda di Anonymus, che vide la condanna del responsabile per accessi abusivi a sistemi informatici. In quel caso il ragionamento decisorio condusse i giudici a conclusioni esattamente opposte, con un severo distinguo tra le finalità ideali perseguite dagli associati e il reato consistito nell'accesso a siti altrui. [11] Bisogna prendere atto che con tutta probabilità siamo in presenza di un mutamento culturale di non scarso rilievo.

Fermo restando quanto affermato poco sopra a proposito della indeterminatezza delle definizioni legislative che favoriscono la libertà degli interpreti nel riempire in modo "creativo" i vuoti lasciati dal legislatore, sta di fatto che se pronunce dello stesso tenore dovessero trovare ulteriori conferme e diffusione, avrebbero quale conseguenza, dall'angolazione della Teoria dei Giochi, di spostare l'equilibrio informativo astrattamente prima considerato, a tutto favore di una delle parti in gioco.

Al riguardo è stato già notato che non esiste nel nostro Paese una causa di non punibilità che sia conseguenza di pretesi comportamenti etici dell'intrusore nel sistema informatico di proprietà altrui, sul modello dei cosidetti "*white hat hacker*", gli hacker buoni, che nella cultura anglosassone si contrappongono ai "*black hat hacker*", animati da cattive intenzioni.

Sta di fatto, ancora, che nelle scarne motivazioni poste a base della decisione del Gip di Catania non viene chiarito ai fini della ritenuta assenza del reato, il collegamento che sarebbe doveroso stabilire tra l'accesso abusivo al sistema privato, la cui realizzazione non è mai stata posta in dubbio, e il *post-factum* rappresentato dalle comunicazioni alla Società proprietaria e quindi dai motivi asseritamente etici posti a base della divulgazione sulla rete dei *bug* riscontrati nel sistema abusivamente violato dall'indagato.

Impossibile non considerare l'impatto di una decisione giudiziale come quella in esame, riguardo all'impegno richiesto agli amministratori dei sistemi informatici sul fronte della protezione delle reti e delle banche dati che su di esse risiedono. Appare palpabile nella lettura di tale decisione l'incertezza, o peggio la svalutazione, dei confini di una nozione come quella di accesso abusivo a sistema informatico che è già frutto di uno slittamento semantico.

La versione giudiziale dell'accesso abusivo, infatti, diluita nell'incertezza dell'hacking etico, si presenta in forme oggettivamente distoniche dalla collocazione dell'art. 615 ter all'interno della sezione dei reati contro l'inviolabilità del domicilio. Nell'orientamento qui considerato è l'idea stessa di domicilio informatico a entrare in crisi o quanto meno ad imporre un serio ripensamento sulla sua reale latitudine anche in sede legislativa.

L' eventualità che una decisione al momento isolata possa trasformarsi in un indirizzo giurisprudenziale, sull'onda emotiva di sensibilità e orientamenti di politica criminale manifestatisi originariamente in ordinamenti diversi da quello nazionale, pone più di un serio interrogativo sulla possibilità del coerente coordinamento della tutela degli hacker in veste di Robin Hood della rete, con la tutela del bene giuridico della sicurezza delle reti e dei dati presentate all'inizio di questo lavoro.

Se da un lato, infatti, l'ordinamento fa carico agli amministratori di sistema di adottare politiche della sicurezza delle cui procedure essi devono rendere conto in maniera capillare, il che evidentemente implica l'adozione di rigidi codici di riservatezza dei protocolli aziendali, dall'altra parte, l'emergere di decisioni giudiziali come quella appena

[11] Corte di cassazione - sezione feriale - sent.16 dicembre 2013, n.50620 la cui massima recita:"Può dirsi sussistente un'associazione per delinquere ex art. 416 c.p. in presenza di un accordo per introdursi abusivamente su siti altrui. La finalità dei valori perseguiti dai componenti, coincidente con principi largamente condivisi nel tessuto sociale, non esclude *ipso facto* la configurabilità di reati associativi". Questo un passaggio significativo della sentenza: "Al di là dei valori ideali, quel che conta è infatti il programma condiviso anche in ordine alle modalità di perseguimento dei fini (per quanto lusinghieri e meritori) che il gruppo si propone: perciò un accordo per introdursi abusivamente su siti altrui - e quello è di norma un reato, a prescindere dalle finalità che animano chi lo faccia - può certamente costituire il presupposto di un'associazione per delinquere".

considerata, favorendo la libera circolazione sulla rete delle informazioni sulle architetture interne dei sistemi informatici, e sopratutto delle loro vulnerabilità, suggerisce "aperture" del tutto opposte.

E' con riguardo a tale riflessione, che evidentemente non è circoscritta al particolare precedente giurisprudenziale preso in esame, ma implica una portata culturale più ampia, che la Teoria dei Giochi, come si è cercato di evidenziare nel corso di questo articolo, diventa un momento ineludibile di confronto e di approfondimento, in grado portare chiarezza in un ambito soggetto a rapidissima obsolescenza, dove l'innovazione tecnologica si accompagna necessariamente a quella concettuale e giuridica.