LA GEOPOLITICA DEL DIGITALE

a cura di Jean-Pierre Darnis e Carolina Polito

Edizioni Nuova Cultura

Ministero degli Affari Esteri
e della Cooperazione Internazionale

Per la realizzazione del progetto (brochure, siti web, pubblicazioni, pieghevoli, manifesti, ecc.), si è usufruito del contributo dell'Unità di Analisi e Programmazione del Ministero degli Affari Esteri e della Cooperazione Internazionale ai sensi dell'art. 23- bis del DPR 18/1967.
Le posizioni contenute nel presente report sono espressione esclusivamente degli autori e non rappresentano necessariamente le posizioni del Ministero degli Affari Esteri e della Cooperazione Internazionale.

Questo lavoro si inserisce nell'ambito delle attività del programma "Tecnologia e relazioni internazionali" dell'Istituto Affari Internazionali (IAI) e beneficia di un contributo da parte della Fondazione Compagnia di San Paolo.

Quaderni IAI
Direzione: Lorenzo Kamel

Prima edizione settembre 2019 – Edizioni Nuova Cultura

Per Istituto Affari Internazionali (IAI)
Via Angelo Brunetti 9 - I-00186 Roma
www.iai.it

ISBN: 9788833652467
Copertina: Luca Mozzicarelli
Foto: © sdecoret / Shutterstock.com
Composizione grafica: Luca Mozzicarelli

Indice

PARTE II. LA GEOPOLITICA DEL DIGITALE: PROSPETTIVE E SFIDE GLOBALI

Autori

Simona Autolitano, Cybersecurity Policy Coordinator, Microsoft.

Cristian Barbieri, Security Specialist, Security and Freedom for Europe (SAFE).

Nicola Bilotta, ricercatore, IAI.

Francesca Bitondo, responsabile di affari istituzionali in Microsoft Italia e Austria, segue principalmente la normativa e policy Ue.

Jean-Pierre Darnis, professore associato Université Côte d'Azur e responsabile del programma IAI "Tecnologia e relazioni internazionali".

Roberta Mulas, professore a contratto di Conflict and Peace Building presso il Dipartimento di Scienze politiche della LUISS e analista di relazioni internazionali e politiche di sicurezza per l'Ufficio Affari diplomatici della Presidenza della Repubblica.

Beatrice Valentina Ortalizio, consulente per Bip. CyberSec, Lead Auditor di Sistemi di Gestione per la Sicurezza delle Informazioni ISO/IEC 27001:2017 e vice curatrice del hub romano dei Global Shapers, un'iniziativa del World Economic Forum.

Alessandro Picchiarelli, sacerdote della diocesi di Assisi e docente di Etica della Tecnologia presso l'Istituto teologico di Assisi.

Carolina Polito, ricercatrice associata, IAI.

Lista degli acronimi

Adm	Armi di distruzione di massa
Afis	Automatic Fingerprint Identification System
Aiea	Agenzia internazionale per l'energia atomica
Ama	Agenti morali artificiali
Arpanet	Advanced Research Projects Agency Network
Bia	Business Impact Assessment
Cert	Computer Emergency Response Team
Cloud	Clarifying Lawful Overseas Use of Data
Csirt	Computer Security Incident Response Team
Darpa	Defense Advance Research Projects Agency
Dg	Direzione generale
Dpia	Data Protection Impact Assessment
Ecso	European Cyber Security Organisation
Enisa	European Union Agency for Network and Information Security
Ep3r	European Public-Private Partnership for Resilience
Epo	European Production Order
Epro	European Preservation Order
Eurodac	European Dactyloscopie
Face	Facial Analysis, Comparison, and Evaluation
Fbi	Federal Bureau of Investigation
Fmi	Fondo monetario internazionale
Fsd	Fornitori di servizi digitali
Gdpr	General Data Protection Regulation
Ia	Intelligenza artificiale
Icann	Internet Corporation for Assigned Names and Numbers
Ict	Information and Communication Technology
Imco	Internal Market and Consumer Protection
IoT	Internet of Things
Ip	Internet Protocol

It	Information Technology
Itr	International Telecommunications Regulation
Itre	Industry, Research and Energy
Itu	International Telecommunication Union
Iva	Imposta sul valore aggiunto
Mad	Mutually assured destruction
Mlat	Mutual Legal Assistance Treaty
Mlps	Multi-Level Protection Scheme
Nato	North Atlantic Treaty Organization
Ncc	Noleggio con conducente
Ngi	Next Generation Identification
Nis	Network Information Security
Nsa	National Security Agency
Nsg	Nuclear Suppliers Group
Ntia	National Telecommunication and Information Administration
Ocse	Organizzazione per la cooperazione e lo sviluppo economico
Osce	Organizzazione per la sicurezza e la cooperazione in Europa
Ose	Operatori di servizi essenziali
Ot	Operation Technology
Ppp	Partenariato pubblico-privato
Salt	Strategic Arms Limitation Talks
Sari	Sistema automatico di riconoscimento immagini
Scada	Supervisory Control and Data Acquisition
Ssnip	Small but Significant Non-Transitory Increase in Price
Start	Strategic Arms Reduction Treaty
Tld	Top-Level Domain
Tnp	Trattato per la non-proliferazione nucleare
Tnt	Trinitrotoluene
Ue	Unione europea
Unicri	United Nations Interregional Crime and Justice Research Institute
Wcit	World Conference on International Telecommunications
Wsis	World Summit on Information Society

Prefazione

Questo volume si pone come obiettivo quello di esaminare le più recenti implicazioni geopolitiche poste in essere dalla rivoluzione digitale. È ormai evidente come la sempre maggiore diffusione dello spazio cibernetico abbia implicazioni per la politica internazionale, l'attività economica mondiale, le relazioni sociali transnazionali, e non ultime le dinamiche geopolitiche globali. Tale diffusione ha permesso infatti a un numero sempre crescente di attori di far emergere con maggior forza le proprie prerogative e le proprie necessità sullo scenario internazionale. Questo volume si propone dunque di tracciare un quadro complessivo dell'evoluzione delle tensioni geopolitiche globali esistenti tra i numerosi attori che popolano ed hanno la capacità di affermare la propria voce nella dimensione digitale, alla luce soprattutto dei più recenti sviluppi in questo ambito, quali, tra le altre, la crescente necessità di progredire nello sforzo normativo per regolare la dimensione digitale, nonché la sempre maggiore tendenza a una territorializzazione del dominio cibernetico in blocchi nazionali, o le implicazioni future date dall'evolversi delle tecnologie quali l'intelligenza artificiale o l'*Internet of Things* (IoT).

A tal fine, questo volume mette insieme esperti provenienti dall'accademia e dal settore privato, con uno sforzo interdisciplinare di vasta portata, per trovare risposte ed idee su come affrontare concettualmente, teoricamente e praticamente le nuove sfide geopolitiche che questi sviluppi comportano.

Il volume è diviso in due parti. La prima parte inquadra la geopolitica del digitale partendo da una disamina dell'evoluzione dello sforzo normativo, principalmente in abito europeo, per regolamentare le attività nello spazio cibernetico. Il capitolo di apertura, di Beatrice Valentina Ortalizio, vuole investigare la definizione di rischio cibernetico al fine di comprendere come la cultura normativa europea stia investendo sulla necessità di valutare tale rischio per implementare misure di sicurezza precise e mirate. Il capitolo si pone l'obiettivo di individuare una metodologia comune e condivisibile di gestione del rischio informatico che aziende e organizzazioni internazionali dovrebbero implementare.

Il secondo capitolo, di Simona Autolitano, si focalizza sulle conseguenze della globalizzazione sul processo diplomatico e, in particolare, su come questa abbia portato ad importanti cambiamenti di equilibri e potere nelle relazioni internazionali. Il capitolo si sofferma su come la cybersecurity rappresenti un'arena emblematica in cui autorità pubbliche e settore privato hanno dato origine a vere e proprie coalizioni che entrano nel processo legislativo, plasmandone il dibattito ed influenzandone le negoziazioni. Prendendo in esame nello specifico le negoziazioni nell'ambito della direttiva 2016/1148, il capitolo analizza come una nuova arena diplomatica, caratterizzata dall'ingresso di *policy network* composti da rappresentanti del settore pubblico e privato, si stia affermando nei giochi diplomatici a livello europeo.

Il capitolo conclusivo di questa prima sezione del volume, scritto da Francesca Bitondo, si focalizza infine sulla proposta del Commissione europea riguardo l'accesso alle prove digitali, il così detto "pacchetto e-Evidence" – insieme ad altre iniziative a livello internazionale quali il Cloud Act e l'ammodernamento della Convenzione di Budapest del 2001 – e vuole sottolineare la tensione geopolitica che la globalizzazione del cybercrimine pone a livello internazionale, la quale vede da una parte la naturale esigenza degli stati a cooperare, sia a livello intergovernativo sia con i nuovi attori coinvolti quali i fornitori di servizi digitali, e dall'altra la volontà da parte degli stessi di mantenere una prerogativa nazionale nella gestione e nell'accesso ai dati in nome di una tutela della sovranità statale.

La seconda parte del volume muove da questo focus sulla normativa europea per affrontare il tema della geopolitica del digitale dal punto di vista delle imminenti sfide e opportunità a livello globale. Il capitolo di Roberta Mulas si pone come obiettivo quello di analizzare in che misura gli strumenti per il contenimento della proliferazione delle armi nucleari possano rappresentare una base adeguata dalla quale partire per contrastare la proliferazione delle armi cibernetiche. Partendo dall'applicabilità della dottrina della deterrenza nucleare, il capitolo prosegue con un'analisi degli strumenti internazionali di non-proliferazione nucleare, soffermandosi infine sul ruolo svolto dagli scienziati nel richiamare a un utilizzo responsabile della tecnologia da loro creata e offrendo quindi spunti di riflessione sulla responsabilità della comunità scientifica nell'affrontare il problema della crescente militarizzazione dello spazio cibernetico.

Nel successivo contributo, Carolina Polito si sofferma sull'evoluzione dell'Internet governance, e si pone come obiettivo quello di analizzare le

direzioni future di tale evoluzione alla luce della sempre maggiore attrattività di un modello di governance alternativo a quello *multi-stakeholder* verso un accresciuta centralità dello stato nazione, sostenuta non solo da attori statali quali Russia e Cina, ma in una certa misura anche da attori tradizionalmente a favore di un ridotto intervento statale nella gestione dello strumento informatico, quali Stati Uniti e Unione europea.

Il capitolo di Cristian Barbieri prende le mosse da un'analisi della gestione quotidiana della sicurezza nelle metropoli, la quale risulta essere sempre più problematica per gli amministratori e le forze di polizia locali che, di conseguenza, sempre più si affidano ad innovazioni tecnologiche per contrastare la criminalità. Il capitolo si propone di descrivere e analizzare i diversi approcci tecnologici delle smart city cinesi, statunitensi ed europee, presentandone successi e fallimenti, senza trascurare il dibattito sul bilanciamento tra diritti fondamentali e finalità di sicurezza.

Il capitolo redatto da Nicola Bilotta è dedicato a un'analisi dei trend e delle implicazioni derivanti dell'ascesa nell'economia globale dei beni intangibili, definiti come risorse e patrimoni non incorporati in beni fisici o in attività finanziarie. Date le loro caratteristiche intrinseche, l'ascesa di tali beni comporta un cambiamento strutturale dei modi di produzione globali che ha sia profondi effetti sulle dinamiche di competizione nei mercati, sia consistenti implicazioni socio-politiche. Il capitolo vuole quindi analizzare le conseguenze di tale cambiamento strutturale dei modi di produzione, al fine di comprendere in che modo gli stati-nazione possano meglio affrontare questa trasformazione.

Il volume si conclude con il capitolo di Alessandro Picchiarelli. L'elaborato vuole indagare il nuovo ambito di riflessione morale, definito algor-etica, nel quale ci si propone di capire che ruolo abbiano gli algoritmi informatici nelle valutazioni morali che l'uomo è chiamato a compiere. Dopo aver esaminato le diverse scuole di pensiero nel dibattito circa l'agentività morale degli artefatti tecnologici, il capitolo vuole infatti contribuire alla riflessione sulle implicazioni morali che la presenza degli artefatti determinano nella vita dell'uomo.

Introduzione

Jean-Pierre Darnis

Associare il termine "geopolitica" al digitale può sembrare impresa ardita. In effetti, la geopolitica porta in sé un riferimento geografico, quello di un'analisi delle dimensioni di potere contestualizzate nel territorio. Per questo motivo la geopolitica ha spesso mostrato dei limiti, diventando a volte il pretesto per sviluppare un pensiero realista piuttosto datato, in quanto molto legato alle frontiere e all'estendersi del dominio del controllo seguendo una logica vestfaliana. Seguendo questo filone può dunque sembrare un controsenso associare una riflessione sulle conseguenze del digitale nella politica internazionale a una riflessione geopolitica, anche perché il digitale del *world wide web* veicola l'idea di un "non territorio", o piuttosto quella di un territorio universale. L'uso del termine geopolitica però non è casuale: nello scenario internazionale si sta difatti in misura crescente assistendo a una serie di sviluppi che tendono verso una territorializzazione del dominio digitale, una dimensione che sembra intrisa di tendenze contraddittorie, fra aperture e chiusure. Ed è per approfondire questa dimensione che abbiamo deciso di promuovere questo volume IAI, per offrire al lettore una serie di analisi che guardano al digitale come a un terreno ricco di poste in gioco politiche, e quindi di contrapposizioni tanto di interessi diversi, quanto di concezioni ideologiche diverse.

Agli albori di Internet c'era la rete Advanced Research Projects Agency Network (Arpanet) la quale metteva in comunicazione i primi "nodi" poggiando sullo scambio di dati tramite pacchetti. Questa si è poi sviluppata attraverso una serie di successive innovazioni promosse dalla mobilitazione congiunta della difesa e della ricerca scientifica per costituire gli elementi di quella che diventerà la rete globale[1]. In quel contesto, senza

[1] Paul E. Ceruzzi, "Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté", in *Le Temps des médias*, Vol. 18, No. 1 (2012), p. 15-28.

ripercorrere l'insieme di queste costruzioni successive bisogna rilevare che, accanto a concetti istituzionali tradizionalmente più chiusi, una visione più aperta prende piede negli Usa, quella che ha spinto i vari scienziati e programmatori a sviluppare uno strumento per la condivisione delle informazioni che fosse il più largo possibile, applicando a un'ambiente sempre più vasto la filosofia della trasparenza e della condivisione fra pari, consustanziale del lavoro scientifico. L'origine storico-scientifica della rete, che si sviluppa fra laboratori e centri di ricerca statunitensi, porta quindi con sé una filosofia di apertura e trasparenza, e un'idea di progresso che poggia sulla maggiore diffusione delle informazioni. Da qui deriva quindi la tendenza tecno-libertaria della rete che corrisponde, in particolar modo, al connubio in essere nell'ambiente californiano di quegli anni, e più specificamente di quello di San Francisco, ove si fondevano la cultura dello sviluppo tecnologico e una contro-cultura libertaria e utopistica, diffidente nei confronti dei centri di potere. L'onda dello sviluppo della rete, e quindi dell'insieme delle tecnologie dell'informazione, diventa dirompente a cavallo fra il 20° e il 21° secolo, diffondendo a livello planetario questo modello tecnologico e politico. La stessa espressione di *world wide web* riassume l'ideale di una comunicazione planetaria senza limiti, l'incarnazione dell'ideale utopistico di villaggio mondiale nel quale l'accesso ai contenuti e la capacità di comunicare in modo universale spalanca le frontiere, attraverso il radicale allargamento delle percezioni e quindi del campo dei possibili individuali e collettivi.

D'altro canto occorre tenere a mente come, fin dall'inizio, le tecnologie digitali siano state tuttavia anche associate alla sicurezza nazionale e alla difesa, politiche per loro natura chiuse all'interno dei confini nazionali. Si deve ricordare che, in primo luogo, la tecnologia Internet è nata con il fine primario di assicurare la continuità della comunicazione anche in caso di attacco nucleare, tramite quella tecnologia di pacchetti di dati e di protocolli che di fatto serviva ad aumentare la resilienza delle reti di comunicazioni. In aggiunta va rilevato che man mano che crescevano gli applicativi di tecnologie dell'informazione, crescevano simmetricamente l'interesse degli organi pubblici e i mezzi da loro dedicati al controllo delle informazioni stesse, ovvero gli organi di spionaggio. Tali organi, se già effettuavano un controllo delle telecomunicazioni analogiche, non soltanto hanno progressivamente aggiornato le loro tecniche sfruttando la tecnologia digitale, ma hanno soprattutto usato alcuni aspetti di questa tecnologia per poter accedere a nuove fonti di informazioni su scala mondiale. Infine, si è inevitabilmente sviluppato anche il necessario paradigma relativo alla

creazione di strumenti di difesa di una rete oggetto in modo sempre più esponenziale di attacchi ostili di varia natura, che richiedono una strategia di protezione da parte di chi deve vigilare l'integrità delle infrastrutture critiche. La centrale importanza di questo aspetto, ha comportato un coinvolgimento crescente delle autorità statali di sicurezza, uniche legittimate a svolgere attività di protezione, controllo e contrasto alle minacce. Questa pratica, tuttavia, ha di fatto contribuito a rinforzare un paradigma della "sicurezza cibernetica" con un forte, se non esclusivo, riferimento nazionale e la crescita di competenze negli apparati statali che rinforzano la preminenza, anche culturale, degli operatori di sicurezza nell'affrontare le tematiche digitali da un punto di vista del potere pubblico.

Abbiamo quindi assistito a una securitizzazione dello spazio cibernetico attraverso lo sviluppo di una specifica sociologia di apparati pubblici all'interno degli operatori della sicurezza dedicati alle attività di "sicurezza cibernetica". Contribuendo a replicare nel mondo digitale la protezione delle frontiere nazionali, la securitizzazione risulta dunque evidentemente in contro-tendenza rispetto alla promessa universalista dello sviluppo digitale. Nel caso europeo, questo sviluppo crea inoltre una serie di impedimenti dati dalle dimensioni e possibilità assai limitate delle risposte statali a fronte delle sfide mondiali che coinvolgono, tra gli altri, anche gruppi industriali di una tale ampiezza da rendere arduo per il singolo stato relazionarsi e contrattare in modo autonomo con questi soggetti.

In contrasto con questa nazionalizzazione dello spazio cibernetico, abbiamo altresì osservato l'evolversi di un'azione congiunta dell'Unione europea. A partire dalle posizioni in materia di antitrust digitale della Commissione europea, la quale ha mostrato una capacità di richiamare all'ordine e multare i colossi tecnologici quando questi si scontrano contro i principi di concorrenza. Si possono inoltre citare l'adozione nel 2018 della direttiva sulla protezione globale e la regolazione dei dati (Gdpr), della direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (direttiva Nis), e del recente Regolamento (Ue) 2019/881 sulla sicurezza cibernetica (Cybersecurity Act). Tali iniziative illustrano l'importante lavoro da parte di una Commissione europea che, su mandato del Consiglio, si mostra attiva colmando di fatto anche i vuoti di competenza e di mobilitazione politica della maggior parte degli stati membri, i quali non sembrano riuscire a stare al passo né con l'evoluzione tecnologica né con le sue conseguenze politiche. La Gdpr è stata discussa per suoi effetti perversi, quali ad esempio la barriera che di fatto rappresenta per le società non europee quando vogliono operare in Europa e viceversa,

nonché per aspetti legati all'organizzazione di un sistema di dichiarazione a volte faticoso. Nondimeno, la Gdpr rappresenta un esempio in larga misura positivo di legislazione europea che non soltanto riempie il vuoto della tutela dei dati personali nel contesto digitale, ma impone anche la forza di un sistema regolatorio europeo collocandosi come riferimento, se non esempio, a livello mondiale. Dal canto suo, il Cybersecurity Act rinforza il ruolo dell'Enisa, l'agenzia europea per la sicurezza cibernetica, aprendo un primo spiraglio circa la possibilità di sostegno operativo agli stati membri e soprattutto conferendole un ruolo chiave nella gestione del nuovo schema europea di certificazione di sicurezza cibernetica. Anche da questo punto di vista, l'Europa si muove sul terreno normativo.

L'approccio europeo può rappresentare un complemento unico a quello statunitense dove la potenza dell'industria digitale e l'attuale indole dell'amministrazione Trump non pongono l'America in prima linea su questi dossier. Tra l'altro con un Parlamento europeo dove crescono Verdi e Liberali dopo le elezioni del 2019, la futura Commissione verrà probabilmente incitata a proseguire e semmai approfondire queste problematiche legate alla tutela del cittadino e della privacy nel contesto digitale. Ciò specialmente in virtù del fatto che la Commissione ha annunciato un ambizioso piano di trasformazione tramite digitalizzazione. L'avvento di una "Commissione digitale" andrà quindi di pari passo con una rinnovata attenzione alla protezione del cittadino e potrebbe costituire quindi un ulteriore modello per la trasformazione digitale degli apparati pubblici e avere ripercussioni dirette sugli stati membri. L'Unione europea, avendo sviluppato una cultura molto attenta alle questioni di privacy e alla salvaguardia dei diritti, potrebbe anche rappresentare un riferimento importante attraverso cui, ad esempio, interpretare l'attuale tendenza "*techlash*" ovverossia la diffidenza verso tecnologie digitali ritenute eccessivamente invasive da un punto di vista della tutela della libertà individuale e della privacy. Questa tendenza è sostenuta dalla convinzione che i vantaggi ottenuti dall'utilizzo di tali tecnologie non ne compensino i difetti, e ha progressivamente condotto alcuni a mettere in pratica l'uscita da applicativi tecnologici, quando non a visioni più radicali di rottura con il contesto digitale. Anche in questo caso le riflessioni critiche nascono in seno all'ambiente tecnologico statunitense, spesso californiano, e sotto alcuni aspetti posso essere viste come una reinterpretazione della vena libertaria che ha caratterizzato l'inizio della "rivoluzione Internet" la quale proponeva una visione positiva e universalista dello sviluppo della rete. In qualche modo infatti dall'utopia dell'aumento illimitato delle possibi-

lità, si è passati a una logica di resistenza e di diffidenza in nome della stessa libertà, il ché alla fine rappresenta soltanto l'illustrazione estrema dello stesso paradigma. La crescita quindi di queste tendenze nel contesto statunitense, unitamente alla preoccupazione per gli aspetti di controllo delle informazioni personali da parte di differenti attori – che stanno emergendo sia in Occidente, come illustrato dal caso Facebook-Cambridge Analitica, sia a livello internazionale, quali il controllo sociale implementato tramite strumenti digitali sperimentato in Cina – crea un contesto di preoccupazione crescente che sta iniziando a produrre sia critiche radicali, il *techlash* appunto, sia volontà di integrazione degli applicativi e sistemi prodotti e/o delle relative norme evidente, ad esempio, negli sforzi normativi dell'Unione sopracitati. Da questo punto di vista occorre, inoltre, evocare il dibattito intorno alle norme valoriali veicolate e sviluppate dagli algoritmi: si tratta di una questione estremamente rilevante nel contesto dello sviluppo delle tecnologie dell'intelligenza artificiale e, anche in questo caso, possiamo osservare diversi trend che si scontrano e che riflettono visioni diverse del mondo. In riferimento alla creazione di nuovi sistemi normativi, infine, occorre sottolineare l'importanza dell'evoluzione dell'uso dei dati digitali nel contesto giudiziario, la cosiddetta *e-Evidence*, che pone una serie di questioni non soltanto da un punto di vista dalla regolamentazione giuridica del dato, ma anche dei rapporti internazionali e del regime di scambi di dati ai fini di procedure di giustizia internazionali.

La tensione che intercorre nei fenomeni descritti tra individuo, sviluppo tecnologico e controllo statale risulta particolarmente evidente se si fa riferimento a un evento storico preciso, quello delle cosiddette "primavere arabe" del 2011. Partendo da un episodio di ribellione contro la polizia in Tunisia, si diffonderà in modo estremamente veloce una mobilitazione contro poteri autoritari in una serie di Paesi del Maghreb e del Medio Oriente, mobilitazione che corre poggiando sulle tecnologie dell'informazione e in modo più specifico su alcuni applicativi di condivisione di notizie tramite telefoni cellulari che scavalcano il classico controllo dell'informazione organizzato da parte dei poteri autoritari per rimbalzare da un Paese all'altro e mettere sotto gli occhi del mondo intero delle dinamiche locali, creando un effetto di diffusione e di legittimazione tramite la mobilitazione di una rete estesa di sostenitori e di informazioni rilanciate da parte dei media tradizionali. In quel contesto, si diffonde quindi l'idea che il digitale assicurerebbe una trasparenza delle informazioni e ridurrebbe i margini di chi non segue le regole del contesto di riferimento, quello

delle liberal-democrazie occidentali. Ma le primavere arabe presentano anche una serie di aspetti che ci aiutano a percepire i limiti della visione tecno-universalista. Prima di tutto queste non hanno determinato cambi radicali di regime, quanto piuttosto la trasformazione di alcuni poteri, con avvicendamenti delle élite al comando. Inoltre, di fronte all'attuazione della censura tramite alcuni applicativi, i poteri nazionali si sono velocemente attrezzati per ridurne i possibili utilizzi da parte dei propri cittadini e controllare, o finanche chiudere, lo spazio cibernetico nazionale. La rivolta egiziana contro il regime di Mubarak, ad esempio, ha portato ad eventi di forte nazionalizzazione dello spazio digitale quali un controllo statale esercitato su domini e contenuti. Queste due tendenze illustrano come la trasformazione democratica tramite la diffusione allargata di informazioni in rete, l'utopia di un modo aperto e trasparente, non sia in larga misura avvenuta in questi contesti. Certamente non bisogna dimenticare la molteplicità di fattori intorno a questi movimenti politici, ma si può certamente osservare che il modello di condivisione universale delle informazioni non ha svolto il ruolo chiave che molti gli conferivano. Al contrario, i movimenti delle primavere arabe e l'uso degli applicativi tecnologici da parte degli oppositori hanno costituito un campanello d'allarme forte per i regimi che desiderano controllare l'informazione e le comunicazioni, i quali si sono quindi affrettati a chiudere le porte dello spazio nazionale.

L'esempio più significativo da questo punto di vista è rappresentato dal caso cinese che sta percorrendo una "via nazionale" al digitale fondata, tra le altre cose, sullo sviluppo di infrastrutture e applicativi cinesi, controllati quindi a vari livelli dalle autorità nazionali. L'ampiezza e la completezza dello sforzo della Cina in materia sta creando di fatto una divisione nello spazio cibernetico mondiale (quantunque non una frammentazione tecnica), fattore ulteriormente aggravato dal contenzioso tecnologico e commerciale con gli Stati Uniti e dalle minacce di embargo che spingono ulteriormente i cinesi a "fare da sé". Da questo punto di vista il recente dossier 5G-Huawei-ZTE offre una serie di spunti estremamente interessanti che dimostrano la complessità intorno alla posizione americana che, sospinta da dichiarati legittimi motivi di sicurezza a fronte di una Cina che ha spesso copiato le tecnologie occidentali per trarne vantaggio competitivo nei confronti dell'Occidente, vuole riaffermare una supremazia politica, tecnologica e commerciale ma che allo stesso tempo rischia di spingere ulteriormente a una nazionalizzazione del web, o piuttosto alla crescita di blocchi che possono diventare stagni se non antagonistici, con l'emergere di fatto di un "blocco cinese." Tale blocco potrebbe

allargarsi in misura rilevante a quei Paesi che scelgono, o sono costretti a scegliere in nome di una dipendenza economica e/o politica, le tecnologie e gli applicativi cinesi. Esiste quindi il rischio concreto del rafforzamento di una partizione in due o più blocchi, idea sostenuta anche dall'esempio dei casi russi o indiani, o da quello dell'Unione europea la cui strategia in campo cibernetico potrebbe divergere da quella statunitense. Rischio che è stato avallato peraltro da una discreta letteratura circa la plausibilità di tracciare un'analogia storica con il periodo della Guerra Fredda e la divisione tra Usa e Unione Sovietica in sfere di influenza. Assistiamo quindi a un paradosso assai violento, quello dell'accelerazione della competizione del campo digitale ma anche quello delle divergenze politiche e normative fra "potenze digitali", in piena contraddizione con l'iniziale promessa universalista, di matrice occidentale, nella direzione di una crescente affermazione delle sovranità nazionali nello spazio cibernetico mondiale.

Nell'ambito di questa potenziale frattura del mondo digitale possiamo anche distinguere fra attori privati e pubblici, e interrogarci su come il rapporto tra essi possa mutare a seconda delle zone di riferimento. Il mondo digitale è stato fino ad oggi fortemente condizionato dalle aziende statunitensi, la maggior parte delle quali californiane, che a partire dai produttori di hardware fino allo sviluppo di applicativi e di piattaforme di social media hanno accompagnato e condizionato l'evoluzione delle tecnologie e delle mutazioni sociali, economiche e politiche ad esse legate. Ragionando sull'esempio americano occorre tuttavia distinguere fra le logiche delle varie aziende, difficilmente ricongiungibili in un unico fascio. In aggiunta, è importate sottolineare il ruolo dei poteri pubblici nel rilevare come i rapporti fra questi e le aziende non sia lineare nel caso statunitense. Tali dinamiche sono sensibilmente diverse nel contesto cinese, dove le aziende leader del mercato tecnologico e digitale sono sempre controllate dallo stato, quantomeno attraverso la presenza di almeno un rappresentante del partito popolare cinese all'interno delle aziende nazionali, presenza che favorisce la creazione un blocco piuttosto solido nel programmare e perseguire gli interessi tecnologici e politici nazionali. Vediamo quindi che i colossi delle tecnologie dell'informazione affrontano il mercato secondo schemi diversi, il che tra l'altro ci deve spingere ad interrogare la visione trasmessa da alcune aziende. Oggi, di fronte alla pervasività tecnologica, quasi onnipresente, e alla particolare dimensione moltiplicatrice delle imprese digitali che agisce come un ampliamento all'infinito delle visioni del fondatore, occorre quindi infine anche approfondire l'analisi delle personalità che si trovano a capo di queste strutture.

Un altro contesto nel quale il paragone con la Guerra Fredda potrebbe risultare opportuno è quello della corsa alla "potenza digitale", e in particolar modo della "corsa agli armamenti cyber", con la quale si intende la competizione per lo sviluppo e il controllo di armi cibernetiche, una dimensione preoccupante specialmente per le difficoltà di controllo delle fonti di produzione e della proliferazione. Per questo motivo, si deve anche pensare ad interrogare il bagaglio di esperienza internazionale nel campo della non-proliferazione per capire se si possono mutuare norme applicabili nel contesto cibernetico. Specialmente in virtù del fatto che accanto ai due Paesi considerati come fonti principali di attacchi, la Russia e la Cina, constatiamo la crescita delle capacità cibernetiche da parte di un insieme di Paesi, si pongono spesso come antagonisti nei confronti dell'occidente, come nel caso della Corea del Nord. In questi contesti abbiamo di fatto una differenziazione rispetto alla visione occidentale, che si traduce non solo nell'inasprimento delle relative posizioni militari ma anche nell'accrescersi delle tensioni intorno al miglior modello di governance della rete. Tra l'altro il concetto stesso di "Occidente" nel contesto cibernetico può risultare abbastanza astratto. Esso corrisponde infatti all'uso che ne viene fatto in un quadro che era quello di un'alleanza come quella transatlantica, alleanza che poggia sulla condivisione di interessi e di strumenti fra le democrazie occidentali. Oggi però possiamo osservare delle tendenze centripete che lasciano adito a dubbi sul concetto di alleanza, e dove la minaccia cibernetica gioca un ruolo in quanto sollecita la tenuta stessa delle istituzioni. La solidarietà in caso di attacco, l'articolo 5 del trattato con riferimento al dominio cibernetico sono, ad esempio, dei temi che dovrebbero essere trattati in modo più sistematico nel contesto dell'alleanza atlantica.

Infine, in linea con le descritte tendenze alla nazionalizzazione dello spazio cibernetico, possiamo notare come, anche in ambito di difesa, sebbene le minacce siano trasversali, mondiali, le risposte rimangono per lo più nazionali. Ciò lascia "a bordo strada", per il momento, le organizzazioni internazionali e il multilateralismo. Uno degli aspetti più stimolanti non soltanto per lo studio ma anche per gli indirizzi di *policy* sta nel necessario rinnovamento di tali strumenti multilaterali, come anche nella possibilità di creare geometrie variabili di eventuali blocchi in via di costituzione. Da questo punto di vista, l'Unione europea potrà risultare di grande interesse se saprà da una parte favorire gli investimenti in tecnologia e dall'altra rafforzare il proprio ruolo regolatore e normativo. Nell'ambito di una diplomazia cibernetica mondiale, l'Unione europea si

trova già all'avanguardia e può aspirare a un ruolo decisivo accanto a Stati Uniti e Cina, a condizione di riuscire però a conciliare le legittime pretese dei singoli stati membri in riferimento alla propria sicurezza nazionale con un rafforzamento degli strumenti dell'Unione, siano questi tecnici o legislativi. Da questo punto di vista possiamo ben sperare in un'azione trasformativa derivante dalla digitalizzazione dell'Unione, intesa non soltanto come messa a livello tecnologico ma anche come progresso dello strumento politico e amministrativo. Tale architettura digitale permetterebbe infatti di trasporre negli sviluppi tecnici e organizzativi l'attenzione per la protezione dei diritti del cittadino e per la salvaguardia della democrazia. La spesso vituperata Commissione europea può, in questo contesto, accrescere il suo peso, anche perché si tratta della creazione di nuove sovranità sul dominio cibernetico che non vengono sottratte al livello nazionale, dove quasi mai sono state prese in considerazione. Un'evoluzione in questo senso, garantirebbe una maggiore tutela dei cittadini europei nello spazio cibernetico mondiale, e andrebbe a colmare i vuoti lasciati da stati-membri in larga misura assorbiti dai loro giochi di politica interna, determinando le capacità future dell'Unione, potenzialmente tanto dirompenti quanto lo è l'evoluzione delle tecnologie e dell'informazione. Anche in una lettura squisitamente geopolitica, esistono modi per non finire schiacciati fra le grandi potenze digitali, Stati Uniti e Cina, sviluppando ulteriormente gli strumenti dell'Unione: il digitale rappresenta quindi un'opportunità per l'affermazione del peso geopolitico dell'Europa.

PARTE I
LA GEOPOLITICA DEL DIGITALE: LA NORMATIVA EUROPEA

1.
Dal cyberthreat alla cybersecurity. La normativa europea e l'emergere di una cultura della gestione del rischio cibernetico

Beatrice Valentina Ortalizio

Nel corso dell'ultimo decennio, si è affermato con sempre più convinzione il paradigma per cui la sicurezza informatica, o cybersecurity, costituisca l'ultima sfida globale che coinvolge individui, aziende, stati ed organizzazioni internazionali. Definirla una sfida presupporrebbe un piano articolato di contromisure che, qualora implementato, sia in grado di superare la componente problematica conducendo l'illuso malcapitato verso il traguardo finale, libero da qualunque preoccupazione.

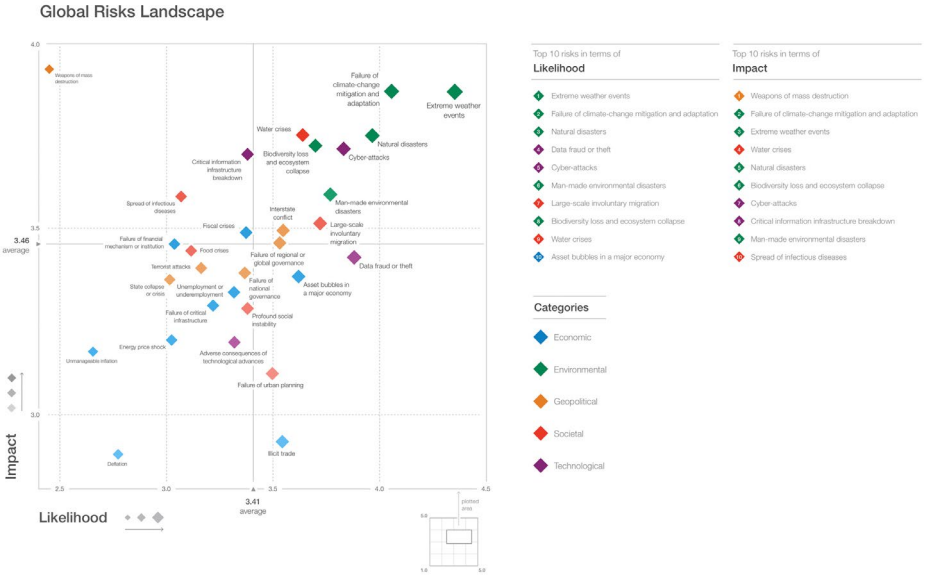
La sicurezza informatica non è *una* sfida, né certamente è *la* sfida del XXI secolo.

La premessa principale di questo capitolo è che la sicurezza informatica costituisce un tragitto: una strada verosimilmente molto articolata che prevede diverse intersezioni e, decisamente, nessun traguardo, piuttosto forse delle tappe "positive" che, se completate, non azzerano del tutto il cammino fin lì percorso, ma di certo no, non una sfida in sé. Quello che per la società 4.0[1] costituisce invece una minaccia concreta e problematica sono gli attacchi cibernetici, identificati nei dieci rischi più probabili e a più alto impatto dal rapporto Global Risks realizzato anche quest'anno dal World Economic Forum[2].

[1] Klaus Schwab, *Shaping the Fourth Industrial Revolution*, Geneva, World Economic Forum, 2018.

[2] *The Global Risks Report 2019*, 14 ed., Geneva, World Economic Forum, 2019, p. 5, https://www.weforum.org/reports/the-global-risks-report-2019.

Figura 1 – Global Risks Landscape



Fonte: *The Global Risks Report 2019*, cit., p. 5.

È il rischio cyber la vera minaccia che individui, aziende, stati ed organizzazioni internazionali sono chiamati a fronteggiare nella nuova era dominata dall'industria 4.0.

L'esigenza di creare nuovi modelli di business per aumentare la produttività delle industrie ha portato a una generale tendenza verso l'automazione, l'informatizzazione, la virtualizzazione, il cloud e verso tutte le funzionalità presenti su mobile. L'insieme di queste caratteristiche definisce l'industria 4.0 a cui le varie componenti sociali sono chiamate a rapportarsi e su cui agisce il rischio dei cyber attacchi.

Scopo di questo capitolo è investigare la definizione di rischio cibernetico e comprendere come la cultura normativa europea sta investendo sulla necessità di valutare il rischio cibernetico per implementare misure di sicurezza precise e mirate.

Per procedere in sincronia rispetto alla direzione che le istituzioni europee hanno intrapreso, l'obiettivo finale è dunque quello di presentare una metodologia comune e condivisibile di gestione del rischio informatico in ambienti It, Ot e IoT[3] che aziende e organizzazioni internazionali dovrebbero implementare.

[3] Ai fini di questa analisi, prenderemo in considerazione indistintamente i tre domini della cybersecurity e dunque la tecnologia dell'informazione (It) ovvero le tecnologie usate

1.1 Definire il rischio cibernetico

Si definisce rischio informatico[4] il prodotto scalare tra la gravità (impatto) delle conseguenze che un evento cibernetico determinerebbe e la probabilità che tale evento pericoloso (minaccia) si realizzi e dunque:

$$R= I \times P$$

I rischi vengono dunque valutati determinando l'entità dei danni potenziali sul sistema che la minaccia potrebbe provocare in caso di suo accadimento, considerando la probabilità che la minaccia causi sempre il maggior danno possibile al suo verificarsi. Le conseguenze della stessa sul sistema dipendono anche in larga misura dal valore dei beni interessati e l'esame delle conseguenze per ogni tipo di minaccia rappresenta un altro aspetto dell'analisi del rischio. Il livello di rischio cibernetico è sempre da considerarsi infatti come una relazione tra il rischio stesso e la valorizzazione dell'asset informatico associato.

Per ciò che concerne gli obiettivi di questo capitolo, le tipologie di minacce verranno intese come agenti potenzialmente malevoli sulle caratteristiche principali per la sicurezza delle informazioni[5]:

- *Riservatezza* – Capacità di garantire la confidenzialità delle informazioni trattate e scambiate con più destinatari;
- *Integrità* – Protezione dei dati e delle informazioni nei confronti delle modifiche accidentali o volontarie del contenuto, da una terza parte;

---

per creare, memorizzare, manipolare e trasmettere l'informazione nelle sue molteplici forme; la tecnologia operativa (Ot) che consiste nei sistemi hardware e software utilizzati nelle operazioni di monitoraggio e controllo dei processi industriali; l'Internet delle cose (IoT), il dominio di più recente identificazione, che include oggetti dotati di sensori e microprocessori che monitorano l'ambiente in cui si trovano, elaborando e comunicando tali informazioni con altri oggetti.

[4] Le definizioni di rischio cibernetico date dalla comunità scientifica sono numerose ed è doveroso precisare che accanto alla combinazione delle conseguenze di un evento e della verosimiglianza del suo verificarsi, la norma UNI ISO 31000:2018 *Risk management - Guidelines*, in italiano *Gestione del rischio - Linee guida*, definisce il rischio come l'effetto dell'incertezza sugli obiettivi.

[5] Secondo la norma ISO/IEC 27002:2013 *Information technology - Security techniques - Code of practice for information security controls*, a queste tre principali si aggiungono anche altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità.

- *Disponibilità* – Attitudine di un sistema ad essere in grado di svolgere una funzione richiesta in determinate condizioni ad un dato istante (es. fornire un servizio ad un utente) o durante un dato intervallo di tempo.

La necessità di proteggere queste caratteristiche delle informazioni risponde all'esigenza di proteggere le informazioni ritenute importanti per il proprio business da individui, stati, organizzazioni e aziende. Per i singoli si pongono problematiche relative a furti di identità e di proprietà intellettuale, ma anche a danni economici, reputazionali e legali se soggetti a vincoli amministrativi. Garantire la realizzazione e il mantenimento del livello competitivo sul mercato protegge invece le strategie aziendali che devono spesso confrontarsi non solo con la possibile perdita di profitto, ma anche, e soprattutto, con la costante esigenza di mantenere stabile la continuità operativa del business e l'erogazione dei servizi per la soddisfazione del cliente. L'esigenza di proteggere la sicurezza delle informazioni diventa più urgente nel caso di organizzazioni sovranazionali e Stati considerati responsabili della sicurezza fisica degli individui presenti sul loro territorio. Questi ultimi devono sottostare alla legislazione internazionale e sono deputati alla protezione degli asset critici del sistema Paese.

1.2 Dal GDPR al Cybersecurity Act: il processo di gestione del rischio nella normativa europea

La portata, la frequenza e l'impatto degli incidenti a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi presenti all'interno dell'Unione europea. Possibili incidenti sono in grado di impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia degli stati. A seguito dell'ingente aumento nel numero e nella qualità degli attacchi cibernetici, l'esigenza di difendere le infrastrutture critiche ha infatti comportato l'urgenza all'interno della legislazione europea di identificare *modus operandi* condivisi per stimolare le aziende a soffermarsi sulla valutazione del rischio cibernetico dei propri asset, specie se critici per la sicurezza nazionale.

La valutazione del rischio è comunemente considerata la prima fase di un più complesso processo di gestione del rischio che, come vedremo in seguito, definisce delle soglie di accettabilità ed eventualmente un piano

di trattamento per i rischi riscontrati. Il processo di risk management per la sicurezza informatica rientra in un più ampio processo di gestione del rischio inerente che ogni azienda dovrebbe operare per valutare la propria esposizione a qualunque potenziale minaccia per il proprio business. Il processo di gestione del rischio *cyber* analizza appositamente le minacce informatiche (e non) che agiscono invece sugli asset informatici e ne impattano l'efficienza in termini di confidenzialità, disponibilità e integrità. Nel corso del capitolo sarà dunque delineato come gli ultimi sviluppi della normativa europea abbiano affermato la necessità per ogni azienda di elaborare un piano di *cyber risk management*.

1.3 Il Gdpr e la valutazione d'impatto privacy

Il Regolamento generale sulla protezione dei dati (Gdpr)[6] è entrato in vigore in tutti gli Stati membri dell'Unione nel maggio 2018. Nel corso dell'ultimo anno, l'opinione pubblica e la comunità accademica hanno ampiamente trattato le novità introdotte in termini di certezza giuridica, armonizzazione e maggiore trasparenza per i dati personali all'interno dell'Ue. Gli utenti sono stati sovraccaricati di centinaia di e-mail che informavano sul cambio di normativa e che invitavano all'accettazione del trattamento previsto per i dati personali. Le novità del regolamento possono essere riassunte in qualche punto: ha sistematizzato l'esigenza di regole più chiare su informativa per la privacy, consenso e limiti al trattamento automatizzato dei dati personali, ponendo nuove basi legali per l'esercizio di nuovi diritti. Vengono inoltre definite nuove figure cardine e tempistiche per il trattamento dei dati, criteri rigorosi per il trasferimento degli stessi al di fuori dell'Ue e sanzioni imponenti nel caso di mancato adempimento agli obblighi prescritti.

Ai fini di questa ricerca, l'analisi delle misure previste dal nuovo Gdpr è imprescindibile nella misura in cui si rivela essere la prima – e al momento ancora unica – legge europea che preveda l'obbligo di effettuare una valutazione di impatto sulla protezione dei dati (*Data Protection Impact Assessment*, Dpia) per stimare i potenziali danni sulla privacy da parte di

[6] Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679.

un processo, sistema o componente informatica che elabora o custodisce dati personali.

La valutazione di impatto sulla protezione dei dati personali è parte del processo di gestione dell'impatto sul business (*Business Impact Assessment*, Bia), che costituisce una delle prime fasi del processo di gestione del rischio che verrà meglio descritto in seguito. Nello specifico, quello che il Gdpr propone e obbliga le aziende ad operare è un esame concreto e giustificato dei rischi relativi alle attività di trattamento delle informazioni, che possono causare impatti negativi sui diritti e le libertà delle persone[7].

Il Regolamento non richiede la realizzazione di una valutazione di impatto sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche. La realizzazione è bensì obbligatoria soltanto qualora il trattamento possa "presentare un rischio elevato per i diritti e le libertà delle persone fisiche"[8]. Di fatto, si rivela particolarmente importante quando e qualora vengano introdotte nuove tecnologie per il trattamento dei dati (per esempio una nuova piattaforma online o un diverso archivio per la raccolta dei dati). Qualora quindi cambino le modalità di trattare il dato, si rivela fondamentale valutare i possibili impatti su ciò che il dato rappresenta[9].

Benché non obbligatoria per ogni trattamento, i vantaggi dell'operare in ogni caso una valutazione d'impatto sui dati personali restano comunque importanti allo scopo di identificare minacce, probabilità di accadimento e responsabilità per la privacy, soprattutto al fine di mitigare i possibili rischi per le parti interessate nella seconda fase del processo di gestione del rischio.

1.4 La direttiva Nis e l'analisi del rischio cibernetico per le infrastrutture critiche

Nel luglio 2016, Parlamento e Consiglio dell'Unione europea hanno adottato la Direttiva Nis che è stata implementata all'interno dei diversi contesti nazionali nel corso del 2018[10].

---

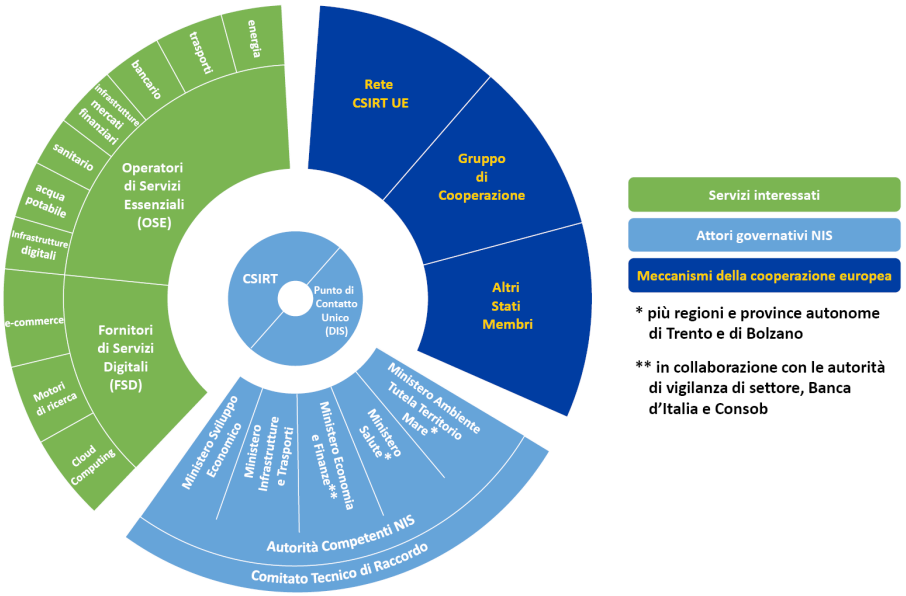
[7] La valutazione di impatto sulla privacy è stabilita dagli articoli 32 e 35 del Gdpr.

[8] Articolo 35 del Gdpr.

[9] Adalberto Biasiotti, *Il nuovo regolamento europeo sulla protezione dei dati*, 2. ed., Roma, EPC, 2016.

[10] Direttiva (UE) 2016/1148 del 6 luglio 2016, recante misure per un livello comune

Figura 2 – Gli attori della Direttiva Nis



Fonte: Sistema di informazione per la sicurezza della Repubblica, *La NIS in pillole*, giugno 2018, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf.

Con la Direttiva Nis, l'Unione europea ha formalmente ammesso che le capacità esistenti non bastano a garantire un livello elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Di fatto i livelli di preparazione negli stati membri sono molto diversi tra loro e questo ha comportato una frammentazione degli approcci. Ne è derivato un livello disomogeneo di protezione dei consumatori e delle imprese che compromette il livello globale di sicurezza delle reti e dei sistemi informativi nell'Unione. La mancanza di obblighi comuni imposti agli operatori di servizi essenziali e ai fornitori di servizi digitali[11] ha reso inoltre finora impossibile la creazione di un mecca-

elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016L1148. In Italia la Direttiva Nis è stata trasposta con il Decreto legislativo n. 65 del 18 maggio 2018: https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg.

[11] All'interno della direttiva si definiscono operatori di servizi essenziali (Ose) gli attori operanti nei settori oggetto della norma e nello specifico energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile e delle infrastrutture digitali. Un operatore fornisce servizi considerati essenziali qualora essi riguardino il mantenimento di attività sociali e/o economiche fondamentali; la

nismo globale ed efficace di cooperazione cibernetica a liùvello dell'Unione.

Per una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi si è reso pertanto necessario un approccio a livello di Unione, che contempli la creazione di una capacità minima comune e di disposizioni basiche in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali.

Secondo la normativa, infatti, identificate le liste di operatori di servizi essenziali con sede nel territorio nazionale per ciascuno dei settori previsti dall'articolo 4 della Nis, le autorità competenti devono provvedere al rilascio delle linee guida per la cybersecurity. L'obiettivo finale è dunque quello di dotare tutti i Paesi dell'Unione di politiche omogenee a riguardo, innalzando i livelli di sicurezza per raggiungere la cosiddetta "cyber resilienza", la costante analisi della capacità di resistenza di fronte alle minacce e la prontezza nel cercare di recuperare lo *status quo* precedente all'evento emergenziale.

Ai fini della presente analisi, la Direttiva Nis assume tuttavia una rilevanza differente per l'accento che pone su diversi punti relativi al rischio cibernetico. Obbliga infatti tutti gli stati ad istituire una strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi che sia in grado di definire: (a) gli obiettivi e le priorità strategiche nazionali in materia; (b) le misure di preparazione, risposta e recupero; (c) l'indicazione dei programmi di formazione in materia; i piani di ricerca e sviluppo relativi alla strategia; (d) l'elenco completo degli attori coinvolti nel processo di attuazione della strategia; (e) il piano di valutazione dei rischi.

Il piano di valutazione dei rischi non è tuttavia richiesto solo in riferimento alla strategia nazionale, bensì la direttiva istituisce l'obbligo di determinazione di un apposito piano di valutazione e gestione dei rischi anche per l'operatività degli operatori di servizi essenziali (Ose) presenti sul territorio. La direttiva individua infatti per gli Ose l'obbligo di valutare la sicurezza della loro rete e dei loro sistemi informativi, operando un'opportuna valutazione del rischio (articoli 14 e 16) connesso alla rilevanza delle loro attività sul territorio nazionale.

---

fornitura di tale servizio dipenda dalla rete e dai sistemi informativi; un incidente abbia effetti negativi rilevanti sulla reale fornitura di tale servizio. La direttiva fa inoltre riferimento ai cosiddetti fornitori di servizi digitali (Fsd) a cui molte imprese nell'Unione si affidano per la fornitura dei loro servizi. Le tipologie di servizi digitali sono individuate nell'allegato III della direttiva e fanno riferimento a servizi online, motori di ricerca, *cloud-computing*.

Tale analisi ha l'obiettivo di individuare le misure tecnico-organizzative adeguate e proporzionate al rischio. Gli attori coinvolti devono inoltre adottare misure adeguate a prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura degli stessi servizi, al fine di assicurarne la continuità. In caso di verifica da parte degli organi di vigilanza (articolo 15) gli Ose devono inoltre fornire all'autorità competente le informazioni necessarie per valutare la sicurezza e le politiche di sicurezza adottate; mentre è compito degli organi di vigilanza verificare l'effettiva attuazione delle stesse, ad esempio mediante attività di audit di sicurezza.

A differenza di quanto previsto per gli Ose, per quanto riguarda gli organi di vigilanza degli operatori di servizi digitali la direttiva non contempla attività di verifica dell'effettiva attuazione delle misure di sicurezza ma richiede agli organi di vigilanza di imporre il rimedio a qualsiasi mancato adempimento degli obblighi di cui all'articolo 16.

Per determinare la rilevanza dell'impatto di un incidente e se sia da considerare sostanziale o meno, si tiene conto di diversi parametri: (i) numero di utenti interessati dall'incidente sul servizio essenziale erogato dal fornitore, (ii) durata dell'incidente, (iii) diffusione geografica dello stesso, (iv) portata della perturbazione del funzionamento del servizio, (v) portata dell'impatto sulle attività economiche e sociali.

La direttiva si propone come un moderato primo tentativo di legislazione europea in materia di sicurezza informatica che si rivela però efficace nel delineare la necessità di implementare per ogni operatore di servizi essenziali un'analisi del rischio strutturata e completa per definire gli impatti e le minacce che agiscono sul proprio contesto per poter mettere in campo misure di protezione specifiche e adeguate alla realtà aziendale in questione.

1.5 Il Cybersecurity Act: certificare il rischio cibernetico

Il Regolamento (Ue) 2019/881[12], conosciuto anche come Cybersecurity Act, è stato approvato a giugno 2019 collocando un altro importante

[12] Regolamento (UE) 2019/881 del 17 aprile 2019, relativo all'Enisa, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione… («regolamento sulla cibersicurezza»), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019R0881.

mattoncino nella complessa costruzione della normativa Ue in materia di cybersecurity. Il regolamento, direttamente applicabile all'interno dell'ordinamento nazionale, parte dal presupposto che la rete e i sistemi informativi siano in grado di aiutare tutti gli aspetti della vita, dando impulso alla crescita economica dell'Unione, oltreché essere fondamentali per il raggiungimento del mercato unico digitale.

Le misure adottate puntano a rafforzare la resilienza dell'Unione agli attacchi informatici e ad accrescere la fiducia dei consumatori nelle tecnologie digitali, creando un vero mercato unico della sicurezza informatica in termini di prodotti, servizi e processi relativi alle tecnologie dell'informazione e della comunicazione (Ict)[13].

In primo luogo, il Cybersecurity Act intende rafforzare il ruolo dell'Enisa, l'Agenzia europea per la sicurezza delle reti e dell'informazione, garantendole un mandato permanente e consentendole di svolgere non solo consulenza tecnica, ma anche attività di supporto alla gestione operativa degli incidenti informatici da parte degli stati membri e rispetto alle loro infrastrutture critiche. In questo modo, il regolamento si rivela complementare rispetto alla Direttiva Nis, consentendo ad Enisa di attuare un sostegno più concreto rispetto al controllo su Ose e fornitori di servizi digitali (Fsd).

Il secondo punto chiave dell'atto legislativo riguarda l'introduzione di un sistema europeo di certificazione della sicurezza informatica dei prodotti e dei servizi digitali. Costituire schemi di certificazione per la sicurezza specifici per prodotti, sistemi e processi Ict si rivela di fatto l'obiettivo principale del regolamento, il cui fine ultimo è quello di facilitare lo scambio degli stessi all'interno dell'Unione, omologando e validando gli schemi già presenti sul territorio.

Ai fini di questa analisi, il Cybersecurity Act risulta importante per l'ulteriore focus legislativo che pone sull'analisi rischio cibernetico. Si legge nel testo come

> per comprendere meglio le sfide nel campo della cibersicurezza e al fine di fornire consulenza strategica a lungo termine agli Stati membri e alle istituzioni, agli organi e agli organismi dell'Unione, l'Enisa ha bisogno di analizzare i rischi attuali ed emergenti connessi alla cibersicurezza.

[13] Luca Tosoni, "Cybersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT", in *Agenda digitale*, 7 giugno 2019, https://www.agendadigitale.eu/?p=47911.

A tale scopo, in cooperazione con gli stati membri e altri enti, Enisa raccoglierà le informazioni pertinenti pubblicamente disponibili o volontariamente condivise, analizzando le tecnologie emergenti e fornendo valutazioni su temi specifici in relazione agli impatti delle innovazioni tecnologiche sulla sicurezza delle reti e dell'informazione, e dunque sulla cybersecurity, dal punto di vista sociale, giuridico, economico e regolamentare.

Enisa sarà inoltre l'organismo deputato ad assistere gli stati membri, le istituzioni, gli organi e le agenzie dell'Unione nell'individuazione dei rischi emergenti connessi alla sicurezza e nella prevenzione degli incidenti attraverso l'analisi di minacce informatiche, vulnerabilità e incidenti. Tra i nuovi compiti di Enisa si pone infatti la necessità di operare un'accurata analisi dei rischi attuali ed emergenti in tema di cybersecurity. Comprendere quali sono i rischi a cui sono esposti non solo gli stati, ma anche le aziende e gli individui presenti sul territorio, definisce un nuovo approccio alla sicurezza verso cui ci si sta pian piano spostando. In una realtà digitale ormai senza barriere all'ingresso, in cui le informazioni si spostano con velocità inimmaginabili fino a pochi anni fa, si rivela infatti fondamentale comprendere le minacce, la probabilità del loro concretizzarsi e i possibili impatti sulle varie caratteristiche della sicurezza delle informazioni attraverso un approccio condiviso da tutti gli stati europei.

Enisa dovrà quindi facilitare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersecurity, quindi alle combinazioni di tutti gli elementi – minacce, probabilità di accadimento e impatto – e sulle possibili misure correttive che potrebbero aiutare gli stati membri ad abbassare il livello di rischio inerente e a rafforzare, in primo luogo, la consapevolezza delle capacità di cyber resilienza e, di seguito, allineando le cosiddette buone pratiche di settore. In questa fase, un fattore determinante per la riuscita del processo è la sensibilizzazione dell'opinione pubblica sui rischi connessi alla cibersecurity attraverso campagne di informazione e fornendo orientamenti ai singoli cittadini piuttosto che a organizzazioni e imprese[14].

[14] In questo contesto si colloca anche l'esigenza di cooperazione dell'Unione con organizzazioni sovranazionali come Ocse, Osce e Nato. Il Cybersecurity Act esplicita infatti al punto 43 che gli sforzi di cooperazione transfrontaliera devono coinvolgere esercitazioni congiunte di cibersicurezza e il coordinamento congiunto di risposta agli incidenti.

1.6 Dalla teoria alla pratica: affrontare e gestire il rischio cibernetico

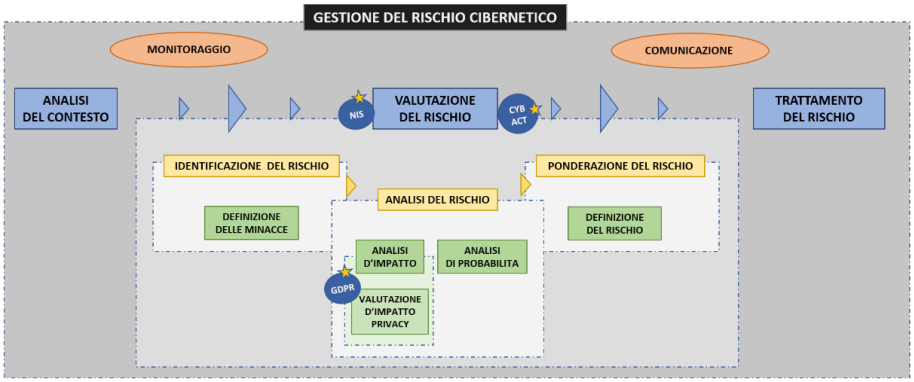
La normativa europea in tema di cybersecurity si rivela ancora abbastanza acerba in riferimento alla definizione di sanzioni approfondite sul tema, tuttavia sono innegabili gli sforzi legislativi per valorizzare l'esigenza per aziende e organizzazioni di operare un'approfondita valutazione del rischio cibernetico.

Come stabilito dalla Direttiva Nis, agli operatori di servizi essenziali e di infrastrutture critiche viene infatti lasciata la libertà di definire le metodologie più efficaci per operare la valutazione dei rischi inerente sia al settore pubblico che a quello privato. Possono essere utilizzate a livelli diversi poiché non esiste una prassi comune e consolidata sulle modalità di applicazione più efficienti. Al momento, la legislazione in materia punta alla promozione e allo sviluppo di buone pratiche per la valutazione dei rischi per incrementare l'utilizzo e l'efficienza di soluzioni interoperabili.

Definiti i vincoli europei in materia di cybersecurity e stabilita l'esigenza di operare una valutazione dei rischi sulla base di questi stessi requisiti, resta da definire quali sono le metodologie consolidate in materia e verso quale direzione si devono muovere gli operatori che intendono affrontare il processo di gestione del rischio cibernetico in maniera strutturata.

Le modalità attraverso cui operare il processo sono indubbiamente numerose. Alle svariate metodologie hanno fatto seguito negli anni molteplici *tool* informatici che, caratterizzati dal settore su cui operano, hanno automatizzato il calcolo del rischio. Ai fini di quest'analisi, verrà presentata

Figura 3 – Processo di gestione del rischio cibernetico



una versione ibrida frutto dell'esperienza pratica con differenti metodologie[15].

Obiettivo di questo capitolo è dunque di individuare gli step basici e comuni a tutte le metodiche per definire e affrontare il rischio cibernetico.

Analisi del contesto – Prima di iniziare, è fondamentale definire una programmazione per comprendere la struttura e il contesto dell'organizzazione su cui si opera. Gli agenti interni sono sostanziali per definire i processi che governano politiche, ruoli, responsabilità, obiettivi strategici, cultura organizzativa, relazioni con le terze parti, asset tecnologici e risorse economiche e di personale. Tuttavia, il contesto esterno dato dai portatori d'interesse con le loro percezioni, valori e aspettative è un valore aggiunto di molte organizzazioni specie se grosse e articolate sul territorio.

Valutazione del rischio – All'interno del framework documentale di gestione del rischio, numerose sono le metodologie realizzate con l'obiettivo di individuare rischi per la sicurezza delle informazioni. La varietà di approcci metodologici differenti è data dalle differenti esigenze progettuali e dai diversi contesti settoriali a cui possono applicarsi. Per quanto le differenti metodologie offrano in ogni elemento un importante spunto di riflessione su come valutare il rischio inerente, l'obiettivo di quest'analisi non è quello di verificare l'efficacia e il merito di una piuttosto che dell'altra, quanto piuttosto quello di definire l'approccio generale da utilizzare nei diversi settori sottoposti alla normative Ue precedentemente descritta.

Identificazione – L'obiettivo della fase di identificazione è di generare un elenco completo dei rischi basato su quegli eventi che possono creare, incrementare, prevenire, degradare, accelerare o ritardare il raggiungimento degli obiettivi strategici aziendali. L'elenco delle minacce può essere più o meno dettagliato, includendo situazioni relazionali che sono – o non sono – sotto il diretto controllo dell'azienda. Questa fase è fondamentale perché le minacce che non sono prese in considerazione inizialmente non faranno poi parte della matrice utilizzata per costruire il rischio asso-

[15] Ci si riferisce in questo caso specifico a: UNI ISO/IEC 27001:2017 *Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti*; UNI ISO 31000:2018 *Gestione del rischio - Linee guida*; COBIT versione 5 - L'infrastruttura aziendale per la governance ed il management dell'IT; NIST 800-39 - Managing Information Security Risk Organization, Mission, and Information System View; lo spagnolo Magerit e l'inglese Cramm (CCTA Risk Analysis and Management Method).

ciato. Le informazioni devono dunque essere aggiornate, pertinenti, provenienti da fonti attendibili e, qualora possibile, derivanti da conoscenze ed esperienze pregresse.

Analisi – Uno stesso evento può avere molteplici conseguenze e può avere influenza su più obiettivi per il business aziendale. La stessa minaccia può avere conseguenze diverse sulla confidenzialità, l'integrità e la disponibilità dell'informazione. Nello specifico, gli impatti su un'azienda, specie se considerata infrastruttura critica, possono essere raggruppati in varie categorie. Qui di seguito si elencano le principali:

- Impatti regolatori: ripercussioni di natura legale che possono nascere dalla mancanza di disponibilità di un servizio, dalla modifica non autorizzata di informazioni, dalle modifiche delle norme di accesso a un ambiente segregato, ecc. che portano l'azienda a incorrere in procedimenti spesso di natura penale o civile per mancato adempimento alla normativa vigente.
- Danno d'immagine: ripercussioni per l'azienda riguardo all'opinione pubblica, stakeholder, clienti finali o fornitori causata da disservizi derivanti da incidenti informatici, difficoltà nell'erogazione dei prodotti o dei servizi, perdita dei dati dei clienti che avevano fatto riferimento all'azienda in questione, ecc.
- Perdite economiche: ripercussioni di natura economica e finanziaria come ad esempio perdite nette sul fatturato, rottura di contratti, mancanza di nuovi clienti, ecc.
- Perdita di efficienza operativa: ripercussioni sull'efficienza e l'efficacia del business aziendale data da malfunzionamenti di servizi, processi o asset che possono portare a minimizzare gli sforzi di produzione dell'impresa.
- Perdita di privacy: qualora si operi una Dpia vengono presi in considerazione gli impatti sulla privacy del soggetto i cui dati possono venir rivelati e che potrebbero essere utilizzati contro di lui a scopo di estorsione.
- Perdita di competitività: implicazioni negative per il commercio che possono causare un accrescimento delle potenzialità dei competitor nel settore di riferimento.
- Danno ambientale: ripercussioni sull'ambiente derivanti da un malfunzionamento dell'impresa o dell'infrastruttura critica (per esempio inondazione, esplosione nucleare, incendio, ecc.).
- Danni alla sicurezza fisica: implicazioni per la sicurezza fisica del personale presente in azienda (si pensi per esempio al personale

di una centrale elettrica in caso di incendio) o dei clienti finali che utilizzano prodotti e servizi compromessi (come avvenuto nel caso dei Samsung Galaxy Note 7 che sono stati ritirati dal mercato dopo casi di esplosione).

Come precedentemente indicato, all'interno della legislazione europea sull'argomento, il Gdpr dedica molta attenzione alle valutazioni di impatto nei casi di perdita di confidenzialità dell'informazione (*data breach*) poiché un'accurata valutazione d'impatto permette alle organizzazioni di conoscere in anticipo le insidie alla privacy di un processo, di un sistema informatico o di un programma, piuttosto che incorrere in sanzioni legali in seguito. Di fatto, la valutazione d'impatto privacy, intesa come parte integrante del più ampio processo di analisi d'impatto, dovrebbe essere più di un semplice controllo di conformità e serve spesso a guadagnare la fiducia delle terze parti con cui l'azienda si raffronta (clienti finali, fornitori, partner) creando relazioni solide.

Le minacce cibernetiche variano a seconda del contesto di riferimento e hanno un impatto afferente a una o più delle categorie precedentemente elencate che agisce su una o più caratteristiche della sicurezza delle informazioni. Definite le minacce e i possibili impatti, non ci sono ancora tutti gli elementi per costruire il livello di rischio. È necessario infatti analizzare i controlli in essere nel contesto di riferimento per comprendere quale è l'effettiva probabilità che una data minaccia si verifichi causando uno o più degli impatti attesi.

Vediamo un esempio pratico.

All'interno di una centrale elettrica, una possibile minaccia da accertare in fase di identificazione può essere data da un'intrusione nei sistemi Scada[16] preposti alla gestione degli allarmi di sicurezza per il controllo di temperatura e raffreddamento delle turbine. La manomissione di questo sistema agirebbe sull'integrità dell'informazione (un cambio di temperatura non autorizzato è di fatto una manomissione sul range di temperatura a cui la turbina dovrebbe viaggiare) e manomettere il sistema di allarme sugli Scada significherebbe non dare visibilità del problema. La modifica dell'integrità di tale valore comporta un impatto sulla sicurezza fisica delle persone presenti nell'impianto in quanto potrebbe scatenare un incendio con conseguenze dolose per il personale d'impianto, ma po-

[16] Nell'ambito dei controlli automatici, l'acronimo Scada (Supervisory Control and Data Acquisition) indica un sistema informatico distribuito per il monitoraggio e la supervisione di sistemi industriali.

tenzialmente anche ambientale se la centrale si trova nei pressi di una foresta che potrebbe prendere fuoco qualora l'incendio si propaghi per qualche centinaio di metri.

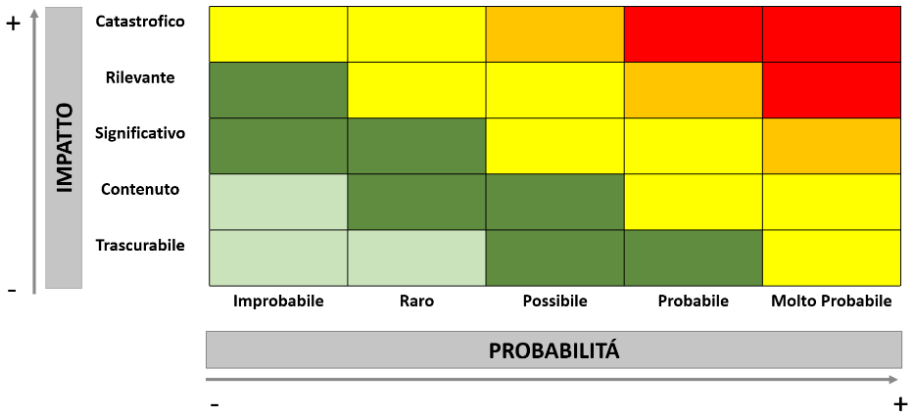
A questo punto, per terminare l'analisi del rischio è necessario comprendere le probabilità di accadimento di questo possibile scenario, dunque i controlli che l'impianto ha messo in piedi per far in modo che questo scenario non si verifichi. I controlli attuabili per la stessa minaccia possono essere differenti e variano a seconda dell'ingenza dell'impatto che si vuole evitare. Nel nostro specifico caso, i sistemi Scada dell'impianto potrebbero essere isolati e non consentire l'accesso alla rete dall'esterno, dunque la rete blindata impedirebbe intrusioni. D'altra parte, tra i vari pro dei software Scada c'è la possibilità di gestire la performance degli impianti in automatismo anche se non si è presenti in loco. Di conseguenza, a seconda della diversità di scenario, si potrà invece utilizzare un meccanismo implementabile sulla turbina che impedisce di far modificare il valore di raffreddamento troppo al di sotto, o oltre, le soglie definite, eliminando la minaccia che questa componente possa essere manomessa. Un'ulteriore intrusione nello Scada impedirebbe però di visionare anche altri eventuali allarmi, di conseguenza questa minaccia nello specifico non sarebbe sanata del tutto.

La definizione dell'impatto e la probabilità di accadimento sono espressione del rischio. I controlli esistenti e la loro efficacia ed efficienza agiscono sulla mitigazione delle possibili minacce ed è per questo motivo che un'accurata valutazione d'impatto aiuta a identificare i problemi precocemente, riducendo i costi del tempo di gestione, le spese legali, mediatiche o d'interesse pubblico, prendendo in considerazione le minacce in anticipo.

Ponderazione – La fase di ponderazione prende in considerazione i risultati dell'analisi combinando i diversi valori che compongono il rischio descrivendo il livello di rischio associato all'organizzazione. Questo risultato è detto rischio potenziale e costituisce il livello di rischio derivante dal prodotto tra l'impatto e la probabilità di accadimento per le minacce identificate, includendo le misure di sicurezza in essere ed escludendo eventuali misure di mitigazione del rischio.

Dopo un'appropriata analisi, in fase di ponderazione, il rischio cibernetico a cui l'azienda o l'organizzazione è esposta si collocherà indicativamente all'interno della seguente matrice (figura 4). La visualizzazione per colori aiuta di fatto a comprendere la gravità del rischio associato.

Figura 4 – Matrice di definizione del rischio



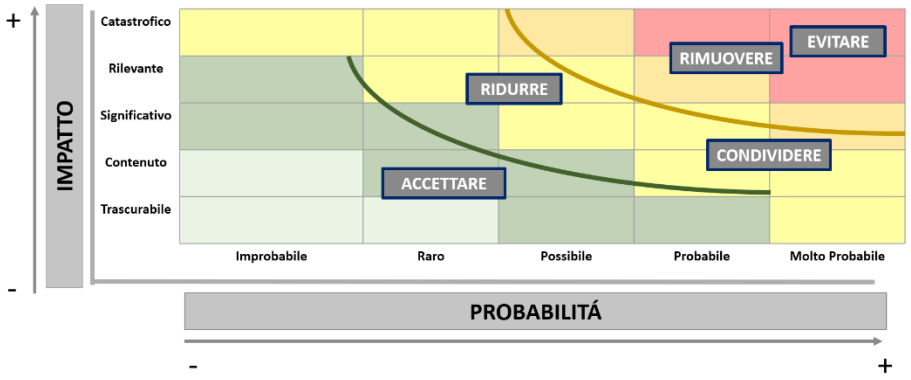
La ponderazione del rischio implica il confronto tra il livello di rischio riscontrato durante il processo di analisi e le minacce definite come applicabili al contesto. Di fatto, l'obiettivo della ponderazione del rischio è di agevolare, sulla base degli esiti dell'analisi del rischio, i processi decisionali riguardo a quali rischi necessitano un trattamento e le modalità attraverso cui attuare le eventuali misure correttive. In alcune circostanze e qualora i risultati siano particolarmente lontani da quelli attesi, in quest'ultima fase si può decidere di intraprendere ulteriori analisi, prendendo in considerazione nuove minacce o elementi di contesto che si erano inizialmente giudicati non applicabili.

Sempre in questa fase si può decidere se procedere o meno con il trattamento del rischio.

Trattamento del rischio – La normativa europea è molto chiara nel suggerire a tutte le imprese e organizzazioni, specie se critiche per esigenze nazionali, di operare un'opportuna analisi del rischio cibernetico. Ciò che resta da appurare è invece l'ultima fase di gestione del rischio.

La fase di ponderazione può prevedere un momento di condivisione con gli stakeholder in cui si decide di non procedere con l'ultima fase di gestione del rischio. Qualora l'analisi sia giudicata completa, ponderata, sufficiente rispetto alle aspettative e con un livello di rischio considerato accettabile per le esigenze dell'azienda o dell'organizzazione, ci si può limitare al completamento dell'analisi del rischio e non procedere al trattamento. In alternativa, l'ultima fase del processo è il trattamento del rischio risultante dal raffronto emerso in matrice durante la fase di ponderazione.

Figura 5 – Scenari di trattamento del rischio



Il trattamento del rischio implica la selezione di una o più opzioni per modificare il rischio associato ed eventualmente abbassarlo fino a un livello di cosiddetto rischio residuo: il rischio che permane dopo l'applicazione di misure di mitigazione al rischio potenziale e che l'organizzazione decide di accettare. Nonostante le misure di mitigazione, un'azienda può decidere di accettare un certo livello di rischio non intraprendendo ulteriori misure di trattamento per diverse motivazioni (investimenti troppo alti, probabilità di accadimento di uno scenario troppo rara, ecc.).

Il processo di trattamento del rischio può prevedere di:

- Accettarlo: il rischio viene dichiarato tollerabile per l'azienda: il rischio inerente coincide con il rischio residuo.
- Ridurlo: l'azienda decide che il livello di rischio è troppo alto e incompatibile con le esigenze aziendali, decidendo quindi di attuare misure che agiscano su una o più componenti del rischio. Queste misure possono comprendere l'eliminazione della minaccia, la modifica della probabilità di accadimento dell'evento impattante o in alternativa delle conseguenze che fanno seguito al verificarsi dell'evento.
- Condividerlo o trasferirlo: l'azienda decide di dichiarare il rischio tollerabile se condiviso con altre parti (partner, ufficio di controllo finanziario o altro) o trasferendolo nei confronti di assicurazioni per il cyber rischio in cui varia l'attribuzione di responsabilità e di costi nel caso in cui la minaccia si verifichi. Le ragioni di tale scelta sono spesso guidate da impatti economici relativi a perdite finanziarie. A volte il rischio cibernetico è considerato accettabile anche se alto perché le eventuali perdite finanziarie vengono condivise

con più parti mitigando le conseguenze per l'azienda suddividendo le eventuali perdite.

- Evitarlo: qualora il rischio per l'azienda sia considerato troppo elevato a causa delle conseguenze ingenti e dell'alta probabilità di accadimento, l'azienda può decidere di non avviare l'attività che comporta l'insorgere del rischio, interrompendo la produzione e non restando sul mercato.
- Rimuoverlo: la teoria accademica della gestione del rischio offre spesso un'ulteriore possibilità per l'abbattimento totale del rischio, la cosiddetta rimozione. Sarebbe anacronistico per le premesse di questo studio suggerire che il rischio cibernetico sia di fatto completamente evitabile. Tuttavia, è corretto considerare che la scelta di rimozione permane anche per il caso del rischio cibernetico secondo alcune condizioni. Ipotizzando uno scenario in cui il rischio sia dato dalla semplice connessione alla rete, una misura di trattamento per l'eliminazione totale del rischio può essere data dalla rimozione della rete aziendale. Certo una soluzione del genere implica un'ulteriore valutazione economica relativamente all'efficienza e alla produttività dell'organizzazione. È un'opzione non facilmente applicabile in tutti i contesti, anzi realisticamente improbabile se comporta una perdita di efficienza nell'operatività dei meccanismi, ma di fatto si presenta come un'opzione anche per il caso del rischio cibernetico.

La scelta dell'opzione di trattamento del rischio cibernetico più appropriata non può prescindere da un bilanciamento di costi e sforzi di attuazione da valutare a seconda dei benefici derivanti e tenendo conto, qualora presenti, dei requisiti cogenti in materia legale, ambientale e di eventuali responsabilità sociali.

Identificata l'opzione verso cui procedere, l'organizzazione è tenuta a realizzare un piano di trattamento del rischio, in grado di comprendere i benefici attesi da ottenere, i soggetti responsabili dell'attuazione, le azioni concrete proposte e le tempistiche entro cui devono essere portate avanti, eventuali vincoli normativi se presenti, costi precisi per le nuove forniture o per ingaggiare più personale e un futuro piano di monitoraggio e valutazione.

Il monitoraggio e il continuo riesame del processo, così come la comunicazione e la consultazione fra le parti coinvolte (fornitori, partner, stakeholder, investitori) sono una parte integrante e sistemica di tutto il processo di gestione del rischio. Devono essere consolidati e avvenire

in maniera continuativa durante tutte le fasi del processo poiché è fondamentale che le esigenze dei portatori di interesse siano ben intese sin dalle fasi iniziali.

La fase finale di monitoraggio offre anche il vantaggio di mettere a disposizione un patrimonio di esperienze, positive e negative, che possono essere utilizzate per il costante aggiornamento non solo dei rischi, ma anche delle modalità di messa sotto controllo. L'azzardo che porta le aziende a non considerare quest'ultimo passaggio necessario comporta che spesso le preziose lezioni, ricavate dall'esperienza, non costituiscono un vettore sufficientemente trainante per analizzare il concreto rischio aziendale. Tuttavia, per assicurarsi che la fase di monitoraggio sia condotta nel modo più fruttuoso possibile, è sempre necessario che le esperienze apprese vengano utilizzate al meglio.

1.7 Creare una cultura della gestione del rischio cibernetico

La normativa europea sulla cybersecurity è entrata in punta di piedi all'interno dell'ordinamento internazionale proponendo un approccio sempre più mirato alle diverse problematiche sollevate dall'avvento di nuove tecnologie e minacce.

Se le premesse a quest'analisi sono state che le sfide alla cybersecurity non sono una battaglia che si può vincere perché non è possibile realizzare difese perfette, le conclusioni del capitolo sono che non è possibile realizzare difese neanche lontanamente soddisfacenti, senza lo studio di un ragionato compromesso fra minacce, impatti e probabilità di accadimento.

Le difese dello spazio cibernetico non sono mai soltanto digitali, impattano la sicurezza logica delle infrastrutture digitali, come quella fisica. L'accesso di personale non autorizzato in un ambiente in cui si maneggiano informazioni confidenziali è una minaccia di sicurezza fisica che impatta potenzialmente la sicurezza logica (il malintenzionato potrebbe copiare su una chiavetta Usb il materiale a cui riesce ad avere accesso essendo entrato in un'area protetta). La presenza di controlli all'ingresso dell'area e password di accesso alle piattaforme contenenti materiale confidenziale sono entrambe forme di controllo di sicurezza fisica e logica che abbassano la probabilità di accadimento della minaccia.

Se in fase di analisi del rischio non si ipotizza che tale minaccia possa

presentarsi, si fa fatica ad individuare quelle che sono le misure appropriate a contrastare la minaccia specifica, che potrebbero essere già in essere o che potrebbe essere necessario implementare in fase di trattamento del rischio una volta riscontrata la vulnerabilità a cui l'ambiente potrebbe essere esposto.

La normativa europea ha suggerito importanti passi verso la definizione di questo approccio al rischio strutturato e normato, ma è sempre importante tenere presenti i limiti dell'analisi del rischio. Come gli specialisti della sicurezza sanno, una buona gestione del rischio non punta a rendere insuperabili le difese, bensì a rendere talmente difficoltosa la consumazione dell'attacco da rendere poco attraente per il criminale l'attacco stesso. La gestione del rischio cibernetico riporta precisamente le stesse dinamiche, aumentandone il valore impattante, qualora siano coinvolte le infrastrutture critiche del sistema Paese. Spesso si sottovaluta l'ipotesi che l'analisi dei rischi informatici venga svolta dai potenziali obiettivi sensibili (aziende, organizzazioni, stati), così come dai potenziali attaccanti. E invece un'azione sbagliata da parte di questi ultimi può comportare vari anni di galera così come guerre internazionali ed è dunque lo stesso criminale a scegliere attentamente il proprio obiettivo, valutando i rischi e le probabilità di successo, decidendo di conseguenza per gli obiettivi considerati più semplici.

La presa di coscienza da parte della legislazione europea sulle diverse componenti del rischio e sulla necessità di operare un'accurata valutazione dei rischi sono elementi costitutivi di una nuova cultura per la gestione dei cyber attacchi che comporta la messa in atto di difese più efficaci che possono condurre l'attaccante a rivolgere la propria attenzione verso altri tipi di obiettivi. L'obiettivo finale di questo studio è dunque quello di incoraggiare la consapevolezza nazionale che la strada verso un comune livello di sicurezza delle reti e dei sistemi informativi è ancora lunga e il percorso verso la cyber resilienza per il Paese è appena iniziato.

Non esistono difese perfette, ma esistono difese efficaci. E soprattutto, esistono modalità concrete per comprendere qual è la propria esposizione ai rischi e decidere quali difese attuare.

2.
Le nuove sfide della diplomazia nell'era della digitalizzazione: la "Direttiva Nis" come caso di studio

Simona Autolitano

Non vi sono dubbi sul fatto che la rivoluzione digitale abbia totalmente cambiato la nostra quotidianità: basti pensare al progresso nello sviluppo degli assistenti personali digitali, all'esplosione dell'IoT, così come alla diffusione di *smart watches* o al recente boom di dispositivi per la *smart home*. Ormai quasi nove famiglie europee su dieci sono online[1] e se da un lato questo livello di connettività crea un'opportunità unica per cittadini ed imprese di tutto il mondo, vi è l'altra faccia della medaglia da considerare.

Come dimostrano recenti attacchi informatici, queste continue novità tecnologiche portano con sé nuovi metodi operativi, nuove interdipendenze, ma anche nuove vulnerabilità e minacce. Prendendo in considerazione soltanto il 2018, le sole imprese europee sono state vittima di oltre 80 milioni di attacchi informatici. Questi attacchi diventano progressivamente sempre più complessi e costano in media ogni anno alle aziende europee 10,3 milioni di euro.

Per far fronte a queste emergenti minacce informatiche, che sempre più colpiscono non solo aziende private, ma anche istituzioni pubbliche e processi democratici, la protezione del ciberspazio è diventata oggi una delle maggiori priorità per i governi di tutto il mondo. Guardando soltan-

[1] Eurostat, *Digital economy and society statistics - households and individuals*, giugno 2019, https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals.

to al periodo 2017-2018 è possibile individuare ben 376 nuove proposte legislative nel campo della cybersecurity in 96 Paesi. In termini di rappresentanza geografica, l'Europa è senza dubbio la regione con il maggiore sviluppo di politiche legate alla sicurezza informatica con il 33 per cento, seguita dalle Americhe con il 30 per cento, Asia con il 23 per cento, Medio Oriente e Africa con il 14 per cento[2].

L'Ue non fa eccezione. Lo sviluppo di un approccio coerente verso la sicurezza informatica a livello europeo risale al 2009, quando l'entrata in vigore del trattato di Lisbona, da cui è derivata un'importante ristrutturazione organizzativa a livello istituzionale, ha permesso una collaborazione senza eguali tra Direzioni generali (Dg) all'interno della Commissione europea. Tali sviluppi hanno portato, nel 2013, alla pubblicazione della prima edizione della "Strategia dell'Ue per la cibersicurezza"[3] e alla proposta di "Direttiva sulla sicurezza delle reti e dell'informazione nell'Unione", nota come Direttiva Nis. Dal 2013 ad oggi lo sviluppo legislativo europeo nel campo della sicurezza informatica è continuato ed annovera ad oggi importanti risultati tra i quali il "pacchetto Cybersecurity"[4] presentato nel settembre del 2017, e la più recente adozione del Cybersecurity Act[5].

Ciò che emerge guardando le diverse iniziative europee è l'idea di cy-

---

[2] Monitoraggio su 18 mesi di politiche legate alla cybersecurity che comprendono politiche legate alla protezione delle infrastrutture critiche e legislazione in materia di criminalità informatica. Microsoft e European Cybersecurity Organisation, *Cybersecurity Awareness Trainings: A Practical Guide*, febbraio 2019, https://www.ecs-org.eu/documents/publications/5c925b318adcd.pdf.

[3] Commissione europea e Alto rappresentante dell'Unione, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro* (JOIN/2013/01), 7 febbraio 2013, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:52013JC0001.

[4] Presentato nel discorso sullo Stato dell'Unione dal Presidente della Commissione europea Jean-Claude Juncker, il "pacchetto" contiene una serie di serie di misure che mirano a rafforzare ulteriormente i livelli di sicurezza informatica nell'Unione. Commissione europea, *Stato dell'Unione 2017 - Cibersicurezza: la Commissione intensifica la risposta dell'UE ai ciberattacchi*, 13 settembre 2017, https://europa.eu/rapid/press-release_IP-17-3193_it.htm.

[5] Parte del "pacchetto", la proposta di Regolamento mira a rafforzare Enisa, l'Agenzia europea per la cibersicurezza, e ad introdurre un nuovo framework per l'adozione di certificazioni di cibersicurezza per le tecnologie dell'informazione e della comunicazione a livello europeo. Si veda: Regolamento (UE) 2019/881 del 17 aprile 2019, relativo all'Enisa, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione… («regolamento sulla cibersicurezza»), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019R0881.

bersecurity come "sicurezza cooperativa"[6]. Tale concetto sottolinea infatti la peculiarità del sistema informatico in cui, anche se gli stati nazionali rimangono gli attori fondamentali nella gestione della sicurezza informatica e nelle trattative diplomatiche a livello europeo, il coinvolgimento di attori non-statali diventa inevitabile.

Numerosi studi hanno approfondito il ruolo dei vari attori emergenti nel campo della cybersecurity. Tuttavia, sono pochi gli studi che si sono focalizzati sul ruolo degli attori non-statali nel processo decisionale. Tali attori meritano un'analisi più approfondita in quanto, comunemente intesi come obiettivi della regolamentazione, questi sono diventati parte attiva e integrante del processo decisionale, cambiando le regole del gioco della tradizionale diplomazia che da sempre ha visto schierati in prima fila esclusivamente attori statali. Pertanto, la seguente ricerca mira ad analizzare la partecipazione del settore privato nello sviluppo delle normative europee in materia di sicurezza informatica, contribuendo così a un nuovo filone di letteratura sul ruolo del settore privato nel processo decisionale.

Guardando al livello europeo, la ricerca si propone dunque di analizzare come il settore privato sia entrato nel processo decisionale e nella tradizionale diplomazia, e con quali effetti da un punto di vista legislativo. Poiché gli attori rilevanti nel ciberspazio sono numerosi, il presente capitolo prenderà in considerazione il settore privato focalizzandosi principalmente su operatori di servizi essenziali e fornitori di servizi digitali, seguendo la definizione della Direttiva Nis[7].

A tal fine, la ricerca si propone di analizzare l'intervento normativo della Commissione europea che ha portato all'adozione della Direttiva Nis, proposta nel 2013 e adottata dal Parlamento europeo nel 2016 con importanti modifiche e aggiunte a livello testuale. Il caso della Direttiva Nis è di particolare interesse in quanto rappresenta la prima vera e propria legislazione europea nel campo della sicurezza informatica volta a regolamentare tutti i fornitori di servizi digitali, indipendentemente dalla loro origine geografica, che offrono servizi nell'Unione. La Direttiva Nis

[6] Gareth Evans, "Cooperative Security and Intrastate Conflict", in *Foreign Policy*, n. 96 (Autumn 1994), p. 3-20.

[7] La Direttiva Nis, adottata nel luglio 2016, include come "fornitori di servizi digitali" le seguenti entità: servizi di cloud computing, motori di ricerca e piattaforme di e-commerce. Si veda: Direttiva (UE) 2016/1148 del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016L1148.

verrà dunque trattata come caso di studio per esplorare il ruolo del settore privato durante i giochi diplomatici.

La raccolta di dati sul processo politico dell'Ue non è un compito facile. Al fine di valutare il ruolo del settore privato durante i tre anni di negoziazione della direttiva sono state condotte interviste con esperti ed attivisti così come un'analisi qualitativa di documenti ufficiali prodotti durante le consultazioni pubbliche e disponibili sul portale della Commissione europea.

Il capitolo verrà suddiviso in tre sezioni principali. La prima mira a concettualizzare l'ingresso del settore privato nell'arena decisionale e a presentare il quadro teorico alla base dell'intera analisi, la seconda sezione introduce lo sviluppo delle politiche europee sulla cybersecurity con particolare attenzione al ruolo degli attori non-statali, ed infine la terza sezione affronta lo studio delle negoziazioni che hanno portato all'adozione della Direttiva Nis al fine di analizzare il ruolo degli operatori dei servizi essenziali e dei fornitori di servizi digitali nell'arena politico-decisionale a livello europeo.

2.1 Sfide diplomatiche fra globalizzazione, tecnologie e nuovi attori emergenti

Paradossalmente l'anno 1961, anno in cui viene ratificata la Convenzione di Vienna sulle relazioni diplomatiche, segnando l'inizio della diplomazia classica corrisponde anche alla fine di quest'ultima. Durante la Guerra Fredda, infatti, si colloca quella che comunemente viene definita come l'ultima fase della diplomazia classica, caratterizzata dall'emergere di istituzioni internazionali e, dunque, dalla transizione delle questioni diplomatiche da un livello puramente nazionale ad uno transnazionale.

Numerosi studi hanno dimostrato come i profondi effetti della globalizzazione e la diffusione di nuove reti di comunicazione – come i social media e le nuove tecnologie – hanno radicalmente/irreversibilmente trasformato i tradizionali canali diplomatici[8].

La rivoluzione delle tecnologie delle comunicazioni e l'avvento di Internet negli anni '60 – alla base del processo di globalizzazione – porta all'emergere di nuovi attori nella politica mondiale e, di conseguenza, alla

[8] Klaus Schwab, "Global Corporate Citizenship", in *Foreign Affairs*, Vol. 87, n. 1 (gennaio/febbraio 2008), p. 107-118.

parallela evoluzione della diplomazia classica, caratterizzata da un graduale declino del principio per cui solo gli stati nazionali hanno il diritto di entrare nell'arena diplomatica.

Secondo diversi studi, l'origine dell'*empowerment* del settore privato – qui interpretato come accesso al policy-making e dunque all'arte della negoziazione – deriva dalla diffusione, a partire dagli anni '80, di partnership tra pubblico e privato (Ppp). È proprio durante quel periodo che l'ondata di privatizzazione diventa mainstream in moltissimi settori, incluso, all'indomani della guerra fredda, quello della sicurezza nazionale[9], il quale venne affidato al/concertato con il settore privato con l'obiettivo di garantire il finanziamento, la costruzione, la ristrutturazione, la gestione o la manutenzione di infrastrutture o di servizi.

Come già notato da Peterson, il settore privato è in grado di fornire conoscenze specializzate e competenze tecniche durante il processo decisionale[10]. A seguito della diffusione di queste partnership tra pubblico e privato, si crea una sorta di interdipendenza dove entrambe le parti ricevono importanti benefici da tali interazioni. Secondo Howard e Jeffrey[11], infatti, entrambe le parti hanno bisogno l'una dell'altra: da un lato, per il settore pubblico lavorare con il settore privato diventa l'unico modo per adempire al proprio ruolo istituzionale e raggiungere necessari obiettivi di politica pubblica – come quello della sicurezza – dall'altro, per il settore privato, collaborare con le istituzioni significa far sentire la propria voce[12]. In particolare, quando vi sono specifici obiettivi di politica pubblica che possono essere raggiunti solo attraverso lo scambio di tali risorse – per esempio la protezione delle infrastrutture critiche – l'emergenza di attori non-statali intorno a specifiche politiche pubbliche porta alla creazione di *policy network*, una sorta di arena in cui settore pubblico e privato interagiscono regolarmente incidendo su importanti decisioni di politica pubblica[13].

È importante prendere in considerazione il fatto che la misura in cui

[9] Fred Schreier e Marina Caparini, "Privatising Security: Law, Practice and Governance of Private Military and Security Companies", in *DCAF Occasional Papers*, n. 6 (marzo 2005), https://www.dcaf.ch/node/12237.

[10] John Peterson, "Decision-making in the European Union: Towards a Framework for Analysis", in *Journal of European Public* Policy, vol. 2, n. 1 (1995), p. 69-93.

[11] Howard E. Aldrich e Jeffrey Pfeffer, "Environments of Organizations", in *Annual Review of Sociology*, vol. 2 (1976), p. 79-105.

[12] John Peterson, "Decision-making in the European Union", cit.

[13] Ibid.

i diversi attori dipendono l'uno dall'altro non è equa[14]. In primo luogo, le coalizioni possono essere in possesso di diverse tipologie di risorse – queste comprendono ad esempio l'autorità giuridica formale, risorse finanziarie, l'accesso ad informazioni, conoscenze tecniche[15]. In secondo luogo, esiste una sorta di gerarchia tra queste. La combinazione tra numero e tipologia di risorse in possesso di una coalizione sono quindi fattori determinanti per l'effettivo potere di influenza delle coalizioni in ambito diplomatico[16].

Oltre alle risorse, i membri di questi network condividono un particolare "sistema di credenze" che consiste di una struttura gerarchica tripartita composta da un *deep core*, nel quale risiedono le convinzioni ontologiche e normative di base, un *policy core* che caratterizza in maggior misura la coalizione e che include i suoi valori e convinzioni circa i nessi causali tra i fenomeni, ed infine alcuni "aspetti secondari" che sono in buona parte contingenti[17]. Una volta formati, basandosi su veri e propri argomenti politici e mostrando un certo grado di attività coordinate nel tempo, questi gruppi entrano i negoziati diventando spesso, come succede a livello europeo, parte formale del processo decisionale[18].

Sebbene governi e istituzioni siano ancora inclini a vederli come indesiderati o persino come intrusi, non vi sono dubbi sul fatto che oggi gli attori non-statali giochino un ruolo di primo piano nella politica mondiale, con conseguenze importanti sulla riorganizzazione dei meccanismi che da sempre sono alla base del sistema internazionale. La globalizzazione ha reso dunque porosi i confini della diplomazia, portando ad importanti cambiamenti di equilibri e potere nelle relazioni internazionali che vedono oggi una maggiore interdipendenza tra business e politica internazionale[19].

---

[14] Ibid.

[15] Chrisotopher M. Weible, "An Advocacy Coalition Framework Approach to Stakeholder Analysis: Understanding the Political Context of California Marine Protected Area Policy", in *Journal of Public Administration Research and Theory*, vol. 17, n. 1 (gennaio 2007), p. 95-117.

[16] Daniel Nohrstedt, "Shifting Resources and Venues Producing Policy Change in Contested Subsystems: A Case Study of Swedish Signals Intelligence Policy", in *Policy Studies Journal*, vol. 39, n. 3 (agosto 2011), p. 461-484.

[17] Paul A. Sabatier, "The Advocacy Coalition Framework: Revisions and Relevance for Europe", in *Journal of European Public Policy*, vol. 5, n. 1 (1998), p. 98-130.

[18] Paul A. Sabatier, "An Advocacy Coalition Framework of Policy Change and the Role of Policy-oriented Learning Therein", in *Policy Sciences*, vol. 21, n. 2/3 (1998), p. 129-168.

[19] Raymond Saner e Lichia Yiu, "International Economic Diplomacy: Mutations in Post-modern Times", in *Discussion Papers in Diplomacy*, 2003, https://www.clingendael.org/node/3625.

2.2 La cybersecurity in Europa: verso l'empowerment del settore privato

Abbiamo visto come l'emergere di attori non-statali nella diplomazia abbia portato nuove sfide a livello nazionale ed internazionale. Difatti l'emerge di nuovi attori, che gradualmente vengono considerati come essenziali per raggiungere importanti obiettivi di politica pubblica, porta inevitabilmente alla questione della rappresentanza di questi ultimi nel processo di identificazione di tali obiettivi.

I *policy network* appena teorizzati sono piuttosto tipici nel modello di sistema di governance europeo[20]. Così come molte altre istituzioni regionali ed internazionali, anche l'Ue ha ampiamente sostenuto la dottrina di partenariato pubblico-privato per soddisfare nuove priorità di politica pubblica, come il raggiungimento della sicurezza informatica.

La digitalizzazione ha progressivamente trasformato tutti i settori della società; se da un lato questa ha offerto numerose opportunità, dall'altro connessioni illimitate espongono la nostra vita quotidiana a nuovi rischi. La consapevolezza di tali vulnerabilità emerge già nei primi anni 2000, ma è solamente con l'attacco informatico avvenuto in Estonia nell'aprile 2007 che il tema della protezione delle infrastrutture critiche diventa oggetto di maggiore attenzione per i governi di tutto il mondo[21].

All'interno dell'Ue tale consapevolezza porta all'introduzione di una serie di nuove misure legislative. L'azione dell'Ue nel campo della cybersecurity può essere descritta con riferimento ai tre obiettivi principali che questa si pone. Il primo, quello della resilienza, vede in primo piano tutte quelle attività legislative legate al raggiungimento di adeguati livelli di sicurezza dei sistemi e dispositivi informatici, così come delle infrastrutture critiche. È qui che collochiamo per esempio l'adozione della Direttiva Nis o il recente Cybersecurity Act. Entrambe queste iniziative mirano infatti ad innalzare la resilienza dei sistemi informatici in tutta Europa attraverso una serie di requisiti minimi di sicurezza o certificazioni europee. Il secondo obiettivo è quello della deterrenza. Se da un lato i sistemi informatici diventano più sicuri, dall'altro è assolutamente

[20] Beate Kohler-Koch e Berthold Rittberger, "The 'Governance Turn' in EU Studies", in *Journal of Common Market Studies*, vol. 44, n. s1 (settembre 2006), p. 27-49.

[21] Myriam Dunn-Cavelty e Manuel Suter, "Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection", in *International Journal of critical infrastructure protection*, vol. 2, n. 4 (dicembre 2009), p. 179-187.

necessario considerare l'aspetto criminale della cybersecurity, mettendo dunque in pratica misure efficaci che possano distogliere i criminali dal compiere un'azione dannosa per timore di importanti conseguenze. Qui collochiamo le recenti attività dell'Ue volte al rafforzamento della cooperazione di polizia e giudiziaria nella lotta alla criminalità informatica come la recente proposta di Regolamento e-Evidence[22]. Il terzo obiettivo infine guarda alla difesa, definita come "dimensione esterna" della cybersecurity. Sebbene una vera e propria strategia connessa alla Politica di sicurezza e di difesa comune nel campo della cybersecurity forse non è ancora stata totalmente realizzata[23], sicuramente vanno notati importanti passi avanti[24].

Guardando ai diversi obiettivi, le azioni rivolte al raggiungimento della resilienza sono sicuramente le più mature. Se da un lato il coinvolgimento dell'Ue diventa necessario per il conseguimento di tale obiettivo – irraggiungibile a livello nazionale – dall'altro l'inclusione del settore privato diventa inevitabile per due motivi in particolare: in primo luogo, la maggior parte delle infrastrutture critiche in Europa sono di proprietà privata e, in secondo luogo, agli attori pubblici mancano competenze tecniche ed expertise nel settore[25]. È nel 2001 che, per la prima volta, la Commissione europea riconosce che la maggior parte dei servizi critici sono ormai offerti da operatori privati[26]. Da quel momento in poi – basti guardare la Comunicazione relativa al programma europeo per la pro-

[22] Commissione europea, *Proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* (COM/2018/225), 17 aprile 2018, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52018PC0225.

[23] La "dimensione esterna" della cybersecurity viene riconosciuta con la prima "Strategia dell'Ue per la cibersicurezza" nel 2013. Tuttavia, per ovvie limitazioni circa la competenza delle istituzioni europee in quest'area, vi sono stati limitati passi in avanti – almeno fino al 19 giugno 2017 con l'adozione da parte del Consiglio dell'Unione europea del "pacchetto di strumenti della diplomazia informatica": *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

[24] Consiglio dell'Unione europea, *Attacchi informatici: ora il Consiglio può imporre sanzioni*, 17 maggio 2019, https://europa.eu/!HG37Kb.

[25] Commissione europea e Alto rappresentante dell'Unione, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro* (JOIN/2013/01), 7 febbraio 2013, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:52013JC0001.

[26] Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM/2001/298), 6 giugno 2001, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:52001DC0298.

tezione delle infrastrutture critiche[27], la prima edizione della Strategia dell'Ue per la cibersicurezza o la Direttiva Nis[28] – l'Ue ha chiaramente evidenziato la necessità di una più stretta collaborazione con il settore privato, basata su "dialogo, partenariato e responsabilità condivisa"[29]. Sebbene la risoluzione del Consiglio del 2009 sia uno dei primi documenti a riconoscere l'importanza di tale partenariato[30], già nella Comunicazione del 2006, la Commissione afferma che il settore privato gioca un ruolo "complementare" nel raggiungimento della sicurezza delle infrastrutture critiche.

Per concretizzare quanto affermato, il coinvolgimento del settore privato diventa gradualmente sempre più istituzionalizzato. Nel 2009 la Commissione lancia una prima piattaforma per promuovere la cooperazione tra il settore pubblico e privato – Partenariato pubblico-privato europeo per la resilienza (Ep3r)[31] – con l'obiettivo di aumentare la cooperazione e la trasparenza, identificare buone pratiche di sicurezza informatica e trovare le migliori soluzioni per proteggere le infrastrutture critiche in Europa. Successivamente, come preannunciato nella strategia per il mercato digitale europeo nel maggio 2015, la Commissione istituisce nel 2016 il primo vero e proprio partenariato europeo pubblico-privato per la sicurezza informatica, dando vita all'Organizzazione europea per la sicurezza informatica (Ecso) con l'obiettivo, tra gli altri, di contribuire a costruire la fiducia tra stati membri ed operatori industriali.

Oltre alla formalizzazione di partenariati tra pubblico e privato, l'organizzazione di consultazioni periodiche con le parti interessate – per

---

[27] Commissione europea, *Comunicazione relativa a un programma europeo per la protezione delle infrastrutture critiche* (COM/2006/786), 12 dicembre 2006, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:52006DC0786.

[28] Commissione europea e Alto rappresentante dell'Unione, *Strategia dell'Unione europea per la cibersicurezza*, cit.; Direttiva (UE) 2016/1148 del 6 luglio 2016, cit.

[29] Commissione europea, *Una strategia per una società dell'informazione sicura – "Dialogo, partenariato e responsabilizzazione"* (COM/2006/251), 31 maggio 2006, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:52006DC0251.

[30] Consiglio dell'Unione europea, *Risoluzione su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione*, 18 dicembre 2009, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32009G1229(01).

[31] Commissione europea, *Proteggere le infrastrutture critiche informatizzate. Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni* (COM/2009/149), 30 marzo 2009, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52009DC0149.

avviare un dialogo, proporre obiettivi e priorità – diventa un passo necessario per il raggiungimento del fine ultimo della sicurezza informatica. Per esempio, nel 2012 la Commissione avvia consultazioni con le parti interessate, in vista della proposta di Direttiva Nis, poi presentata l'anno successivo.

Un'altra modalità di coinvolgimento del settore privato è rappresentata dalla formazione di gruppi di esperti, in grado di contribuire alla definizione di strategie nel campo informatico. Per esempio, con il Regolamento relativo all'Enisa adottato nel 2013, viene istituito il gruppo permanente di parti interessate dell'agenzia con l'obiettivo di creare sinergie tra esperti provenienti dal settore privato e dalle autorità competenti degli Stati membri[32].

Proprio attraverso canali formali ed istituzionalizzati, il settore privato comincia gradualmente ad acquistare una nuova posizione di potere all'interno del quadro europeo. In questo scenario complesso, l'Enisa istituzionalizzata nel 2004, diventa un attore fondamentale nel quadro decisionale ricoprendo il ruolo di *policy broker*, il cui fine ultimo è trovare un ragionevole compromesso, mediando tra le parti[33].

Dunque, le istituzioni europee e il settore privato diventano gradualmente interdipendenti in quanto ognuno ha bisogno delle risorse dell'altro. Competenze e know-how tecnico sono richiesti dalle istituzioni europee, l'accesso all'arena politico-decisionale dal settore privato. Interazioni ricorrenti, consultazioni pubbliche, piattaforme di dialogo e cooperazione a livello europeo, hanno creato opportunità di accesso ai negoziati politici, ma anche contributo alla creazione di *policy network* formati da enti pubblici e privati che danno vita ad attività coordinate nel tempo, in parallelo allo sviluppo dell'agenda digitale europea.

Il ciberspazio rappresenta quindi una nuova arena legislativa, in cui un grande numero di attori entrano nel gioco diplomatico a livello europeo. Pertanto, la sezione successiva esplorerà l'ingresso di queste coalizioni nel dibattito a livello europeo che ha portato all'adozione della Direttiva Nis nel luglio 2016.

[32] Regolamento (UE) n. 526/2013 del 21 maggio 2013 relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (Enisa)…, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32013R0526.

[33] Commissione europea, *Proteggere le infrastrutture critiche informatizzate*, cit.

2.3 La "Direttiva Nis" e l'emergere di nuovi attori nella scena diplomatica europea

Come precedentemente accennato, l'impegno dell'Ue in materia di sicurezza delle reti e dei sistemi informativi risale già ai primi anni del 2000. In particolare, nel 2003 l'Ue riconosce "la dipendenza europea da un'infrastruttura interconnessa nel settore dei trasporti, dell'energia, dell'informazione ed altri, e la conseguente vulnerabilità dell'Europa sotto questo profili"[34]. Da quel momento in poi l'Ue porta avanti una serie di politiche e normative nel campo della sicurezza informatica. Tuttavia, è solo nel 2013 – con l'adozione della "Strategia dell'Ue per la cibersicurezza" e con la proposta di Direttiva Nis – che la legislazione a livello europeo raggiunge un importante grado di maturazione.

La proposta formulata dalla Direttiva Nis punta al rafforzamento della resilienza informatica in tutti i Paesi europei e a una più efficace cooperazione tra autorità competenti. Questi obblighi in materia di sicurezza e di segnalazione di incidenti informatici rappresentano una grande novità, soprattutto per alcuni dei servizi digitali in ambito di applicazione della direttiva.

Come avviene solitamente, prima di proporre nuove iniziative in materia legislativa la Commissione esegue un *impact assessment* – un'attenta valutazione per definire l'impatto che la proposta legislativa potrebbe avere a livello economico e sociale. Ciò è valido anche per la Direttiva Nis, proposta nel febbraio 2013: le relative consultazioni con le autorità pubbliche di diversi stati membri e gli attori non-statali risalgono al 2012.

Tra i rappresentanti del settore privato che hanno partecipato alle consultazioni vi sono fornitori di servizi digitali – per esempio i fornitori di servizi Internet o di cloud computing – ma anche rappresentanti di settori tradizionali come quello bancario e finanziario, energetico, dei trasporti e così via. La modalità di coinvolgimento di tali attori è stata principalmente tramite l'Ep3r, ma anche attraverso l'istituzione di diversi gruppi di esperti, in particolare l'Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids[35], così come tramite riunioni bilaterali.

---

[34] Consiglio dell'Unione europea, *Strategia europea in materia di sicurezza. Un'Europa sicura in un mondo migliore*, 5 dicembre 2003, p. 29, http://europa.eu/!pY34wC.

[35] Dettagli sui lavori del gruppo di esperti sono disponibili nel sito della Commissione: *Cybersecurity of Smart Grids*, https://europa.eu/!Yk66jN.

Se da un lato il 66,3 per cento di coloro che hanno partecipato alle consultazioni era favorevole all'introduzione di un obbligo normativo per la gestione dei rischi legati alla sicurezza delle reti e dell'informazione[36], dall'altro si sono registrate numerose divergenze su punti cardine della direttiva quali l'ambito di applicazione e l'obbligo di notificazione degli incidenti. Queste divergenze erano motivate principalmente dal timore che una maggiore regolamentazione potesse incidere negativamente sullo sviluppo economico e sul mercato europeo, rendendolo meno competitivo rispetto al mercato globale.

Durante tre anni di intensi negoziati, in linea di massima, i principali punti di disaccordo si sono sviluppati attorno a due questioni: l'inclusione dei servizi digitali in quanto operatori del mercato e l'introduzione del concetto di stabilimento principale. Riguardo alla prima questione, la proposta della Commissione di estendere l'obbligo di segnalazione di incidenti informatici significativi includeva inizialmente i "principali fornitori di servizi della società dell'informazione" – come ad esempio servizi di cloud, social media, piattaforme di e-commerce e motori di ricerca – e settori della società generalmente definiti come critici, come il settore energetico, finanziario e bancario, energetico, sanitario, dei trasporti, e l'amministrazione pubblica. Riguardo alla seconda questione, il concetto di stabilimento principale si legava fondamentalmente all'obbligo di segnalazione degli incidenti. Inizialmente infatti la proposta legislativa faceva riferimento a questo nuovo obbligo senza affrontare chiaramente le modalità di tale segnalazione. Dunque, potenzialmente, uno stesso incidente avvenuto in un Paese europeo, ma propagatosi in più di un Paese membro, avrebbe dovuto essere comunicato a diverse autorità competenti. Tuttavia, nel caso di fornitori di servizi digitali, che per definizione offrono gli stessi servizi digitali in più Paesi, tale metodo di notifica degli incidenti risultava poco efficiente. Il concetto di stabilimento principale emerge dunque come soluzione durante le negoziazioni. Sulla base di questo concetto, i fornitori di servizi digitali hanno l'obbligo di notificare gli incidenti presso la propria sede di rappresentanza in un solo Paese dell'Unione, il cosiddetto "stabilimento principale". Saranno poi gli stati membri a dover garantire la cooperazione transfrontaliera delle autorità competenti quando necessario.

[36] Commissione europea, *Commission Staff Working Document Impact Assessment. Accompanying the document Proposal for a Directive … concerning measures to ensure a high level of network and information security across the Union* (SWD/2013/032), 7 febbraio 2013, p. 9, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52013SC0032.

Dopo lunghi negoziati, un primo accordo politico tra Commissione e Parlamento europeo è stato raggiunto nel dicembre 2015, mentre la Direttiva Nis è stata adottata definitivamente il 6 luglio 2016. È interessante notare che il testo adottato nel 2016, se confrontato con l'originaria proposta del 2013 e la posizione del Parlamento europeo raggiunta nel 2015, presenta numerosi emendamenti su alcuni punti essenziali – come l'ambito di applicazione. Per esempio, se il testo originariamente proposto dalla Commissione includeva nuovi settori – piattaforme di e-commerce, portali di pagamento, social media, motori di ricerca, servizi di cloud computing, rivenditori online di applicazioni[37] – quello proposto dal Parlamento europeo li escludeva, mentre con il testo finale del 2016 si torna a una loro parziale inclusione.

L'inclusione nel testo definitivo di solo alcuni dei principali fornitori di servizi della società dell'informazione, definiti come "fornitori di servizi digitali", così come l'inclusione del principio di stabilimento principale, risultano particolarmente interessanti e rappresentano un cambiamento politico-legislativo che merita un'analisi più approfondita.

Inoltre, guardando alle obbligazioni che la direttiva impone a questa nuova categoria di enti, emerge l'applicazione del principio del "*light touch approach*". Sulla base di questo principio, proposto inizialmente dalla Lettonia durante la Presidenza del Consiglio, i servizi digitali sono sottoposti ad un regime differente rispetto agli operatori dei servizi essenziali – sia per ciò che concerne le misure organizzative e di sicurezza, che per la notifica degli incidenti.

La sezione successiva si propone di analizzare il ruolo di questi nuovi attori nella scena diplomatica a livello europeo per spiegare in che misura questi abbiano influenzato tale cambiamento a livello politico-legislativo.

2.4 La formazione di policy network intorno alla "direttiva Nis": credenze, risorse ed influenza

Di fronte a questo nuovo complesso quadro legislativo diversi attori – statali e non – cominciano ad esprimere le proprie posizioni in modo più o meno formale.

[37] Commissione europea, *Proposta di Direttiva recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione* (COM/2013/48), 7 febbraio 2013, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52013PC0048.

Innanzitutto vi sono gli stati membri; essi rappresentano il primo ambito di applicazione della direttiva – ad essi viene richiesto di costituire un gruppo di cooperazione con l'obiettivo di facilitare la collaborazione e lo scambio di informazioni tra gli stati membri, di istituire una rete di Gruppi di intervento per la sicurezza informatica in caso di incidente (Csirt) nazionali al fine di promuovere una cooperazione operativa rapida ed efficace, nonché di dotarsi di strategie nazionali in materia di sicurezza delle reti e dell'informazione.

Il secondo ambito di applicazione riguarda invece gli attori non-statali, i fornitori di infrastrutture critiche e i fornitori di servizi digitali. Questi ultimi rappresentano una novità legislativa in quanto è la prima volta che delle aziende vengono sottoposte a obblighi in materia di sicurezza informatica a livello europeo a prescindere dalla loro origine geografica purché fornitrici di servizi digitali nell'Unione.

Infine, guardando alle istituzioni europee attive intorno a questa proposta legislativa, oltre al Parlamento europeo, in particolare le Commissioni Industria, ricerca ed energia (Itre) e quella per il Mercato interno e la protezione dei consumatori (Imco), vi sono l'Enisa e la Squadra di pronto intervento informatico (Cert-Eu).

Tramite continui scambi di opinioni e informazioni, questi attori cominciano a formare delle coalizioni – o *policy network* – composti da rappresentanti del settore pubblico e privato – contraddistinte dal possesso di particolari risorse e da un "sistema di credenze" ed in grado di entrare nell'arena diplomatica europea.

Guardando al sistema di credenze, possiamo affermare che i vari *policy network* condividono il *deep core* – in cui risiedono convinzioni ontologiche e normative di base. Considerando l'entità del problema, infatti, tutti gli attori, dal settore privato alle organizzazioni non governative e al mondo accademico – concordano sulla necessità di rafforzare la sicurezza dei sistemi e delle reti dell'informazione a livello europeo. L'incremento delle minacce informatiche, nonché le vulnerabilità di Internet, sono infatti comunemente percepite dai diversi attori.

Tuttavia, il *policy core* – valori e convinzioni circa i nessi causali tra i fenomeni, cioè le modalità su come raggiungere al meglio la sicurezza delle infrastrutture critiche – cambia. Da un lato, la percezione circa la necessità di includere infrastrutture critiche – come il settore dell'energia o quello finanziario – è condivisa dai diversi attori, statali e non. Questo in realtà non rappresenta una particolare sorpresa, infatti tali settori sono già altamente regolamentati a livello nazionale, e la Direttiva Nis non aggiunge niente

di più né a livello di misure per la sicurezza, né a livello di segnalazione di incidenti ad autorità competenti. Gli operatori di infrastrutture critiche si sono dunque trovati generalmente d'accordo sulla proposta della Commissione, sottolineando l'importanza di una responsabilità condivisa e di standard di sicurezza minimi a livello europeo data l'interconnessione e l'interdipendenza tra questi settori a livello europeo – se non addirittura globale. Dall'altro, guardando all'ambito di applicazione della direttiva a nuove entità, possiamo identificare due principali scuole di pensiero attorno alle quali si formano ben presto due coalizioni o *policy network*.

Da una parte vi sono coloro che credono nella necessità di un approccio più duro e di regolamentazioni capaci di imporre standard di sicurezza elevati. Secondo questa prima scuola di pensiero, dunque, la direttiva proposta deve includere gli operatori digitali, i cui servizi, forniti attraverso Internet, sono alla base delle principali attività economiche e sociali del Paese, tanto che tali attività o servizi, se sospesi per un paio d'ore, potrebbero avere un impatto significativo sull'intera società.

D'altra parte vi sono coloro che ritengono che tali regolamentazioni potrebbero avere un impatto negativo sullo sviluppo economico e sull'innovazione. Essi ritengono infatti che il costo aggiuntivo complessivo per soddisfare questi nuovi obblighi a livello dell'Ue, il quale risulterebbe a carico di tutti i settori, sarebbe particolarmente elevato e potrebbe dunque avere un importante impatto economico. Inoltre gli stati membri partono da diversi livelli di sicurezza. Per evitare squilibri essi dovrebbero guardare alle specificità dei loro mercati e gradualmente identificare i passi necessari per raggiungere livelli più elevati in termini di capacità e preparazione necessaria per migliorare la sicurezza a livello europeo.

Per quanto riguarda la questione della segnalazione obbligatoria degli incidenti, nella proposta iniziale della Commissione non vi era alcuna spiegazione circa la modalità di notifica e ciò implicava, potenzialmente, la necessità per un fornitore di servizi digitali di dover notificare lo stesso incidente presso più di un Paese membro. Per la loro stessa natura di servizi digitali, infatti, questi vengono offerti in diversi Paesi, indipendentemente dalla effettiva posizione geografica. Intorno a questa questione vi è dunque una prima scuola di pensiero che spinge verso un equo trattamento per entrambe le categorie di servizi digitali e operatori critici; la seconda, invece, richiede l'introduzione del concetto di stabilimento principale per agevolare tali notifiche sulla base della natura stessa di tali operatori.

Intorno a queste "credenze" – composte da *deep core* e *policy core* – diversi attori, statali e non, cominciano a collaborare, mostrando un certo

grado di attività coordinate nel tempo, entrando come parte formale del processo decisionale e nel gioco diplomatico a livello europeo[38].

Tenendo conto delle questioni più rilevanti – ambito di applicazione della direttiva e segnalazione degli incidenti – possiamo individuare due principali coalizioni. La prima annovera, tra le istituzioni europee, l'Imco del Parlamento europeo, alcuni dei Paesi membri più piccoli – come la Slovacchia – ma anche la Svezia, Gran Bretagna, Estonia, Irlanda. All'interno di questa coalizione, collochiamo inoltre i fornitori dei servizi digitali. Questa prima coalizione ritiene che i servizi della società dell'informazione non sono essenziali quanto le infrastrutture critiche e non possono essere paragonati a tali settori. La seconda coalizione riunisce la Commissione europea, Francia, Germania e Spagna tra i Paesi membri più attivi, insieme ad operatori di infrastrutture critiche e società di telecomunicazione, che sostengono l'inclusione di un elenco non esauriente di "servizi della società dell'informazione", affermando quindi la necessità di stabilire requisiti di sicurezza minimi, indipendentemente dalla natura dei fornitori.

Il concetto di stabilimento principale emerge invece in modo più preponderante in una seconda fase delle negoziazioni, una volta definito l'ambito di applicazione. Il problema è che i fornitori di servizi digitali, in quanto tali, offrono i loro servizi in più di un Paese membro. Per questo motivo, la prima coalizione sottolinea l'importanza di tale concetto per evitare ventotto segnalazioni diverse per uno stesso incidente, la seconda continua a sostenere la "parità" di trattamento tra operatori critici.

Non vi sono dubbi sul fatto che queste coalizioni hanno diverso potere di influenza e ciò dipende principalmente dal tipo di risorse in loro possesso. Guardando per esempio all'autorità formale, possiamo affermare che i Paesi più grandi – Germania, Francia e Spagna – hanno generalmente più potere di influenza durante le negoziazioni politiche rispetto a Paesi più piccoli come Svezia, Estonia, o Irlanda. Considerando invece attori non-statali, vi sono in prima linea gli operatori di telecomunicazioni a totale sostegno della proposta della Commissione. Questi, avendo l'appoggio di grandi Paesi europei, hanno un potere di influenza maggiore se paragonati a nuovi attori emergenti, che invece trovano l'appoggio di Paesi più piccoli come la Svezia, l'Estonia o l'Irlanda.

Vi sono inoltre "aspetti secondari" da non sottovalutare[39]. In tutta que-

[38] Paul A. Sabatier, "An Advocacy Coalition Framework of Policy Change…", cit.

[39] Paul A. Sabatier, "The Advocacy Coalition Framework: Revisions and Relevance for Europe", cit.

sta discussione, emerge una certa criticità dell'opinione pubblica verso i fornitori di servizi digitali. Leggendo i giornali o guardando i social media, emerge infatti un pensiero comune verso la non volontà dei grandi giganti di collaborare insieme per raggiungere un più elevato livello di sicurezza.

Nonostante la diversità di interessi tra i vari attori coinvolti nelle coalizioni – statali e non – questi attori cominciano a cooperare: da un lato Paesi come la Svezia o l'Estonia trovano il supporto dei fornitori di servizi digitali e viceversa, dall'altro gli operatori di infrastrutture critiche trovano il sostegno in Paesi come Francia, Germania, Spagna e viceversa.

Enisa emerge come *policy broker* cercando di mediare tra le parti, trovando nella Lettonia un importante alleato. La Lettonia, infatti, durante la Presidenza del Consiglio introduce un compromesso importante che dà una svolta alle negoziazioni: il concetto di *light touch approach*. Come sostenuto dalla prima coalizione, i fornitori di servizi digitali sono meno critici rispetto agli operatori dei servizi essenziali e dunque possono essere regolati tramite un approccio normativo più "leggero". Tuttavia, come sostenuto dalla seconda coalizione, anche i fornitori di servizi digitali sono richiesti di notificare gli incidenti che hanno un "impatto sostanziale", definendo però soglie diverse rispetto agli incidenti da notificare per gli operatori dei servizi essenziali.

Dunque, nel contesto della Direttiva Nis, vediamo una collaborazione senza eguali tra attori statali e non che porta questi ultimi a entrare nell'ambito delle negoziazioni come fossero quasi veri e propri "stati membri", riuscendo a influenzare il risultato legislativo finale.

2.5 Riflessioni finali: verso una democratizzazione della diplomazia?

L'idea di cybersecurity come "sicurezza cooperativa" emerge chiaramente nel contesto europeo con conseguenze importanti per le relazioni internazionali. Tale concetto sottolinea infatti la peculiarità del sistema informatico in cui, anche se gli stati nazionali rimangono gli attori fondamentali nella gestione della sicurezza informatica e nelle trattative diplomatiche, il coinvolgimento di attori non-statali diventa inevitabile.

Diversi studi hanno dimostrato come i profondi effetti della globalizzazione e la diffusione di nuove reti di comunicazione – come i social media e le nuove tecnologie – hanno portato all'emergere di nuovi attori nella politica mondiale. Guardando ai domini di guerra come definiti dalla

Nato il ciberspazio, decretato come quinto dominio di guerra nel 2015, si distingue chiaramente dagli altri (aria, terra, mare e spazio), essendo creato ed operato da attori non-statali. Questa sua peculiarità di spazio interconnesso porta all'inevitabile necessità di collaborazione e partecipazione con tutti gli attori coinvolti.

Vi sono diversi studi che guardano al ruolo del settore privato nel campo legislativo. Tuttavia, questi si soffermano principalmente sulla questione normativa e cercano di rispondere al quesito circa la positività o meno di tale cooperazione. Vi sono infatti diverse scuole di pensiero circa la creazione di partnership tra pubblico e privato. Se da un lato, l'inclusione del settore privato è considerata positiva per molte ragioni – expertise, conoscenze tecniche, efficienza e flessibilità; dall'altro, la partecipazione del settore pubblico al processo decisionale porterebbe ad una distorsione degli obiettivi politici e a una frammentazione a livello operativo.

Pertanto, il presente capitolo si è proposto di analizzare il processo di *empowerment* a favore del settore privato – qui interpretato come opportunità di accesso al *policy-making* e all'arte della negoziazione – evitando di guardare all'aspetto normativo della questione.

Fino ad oggi sono state condotte numerose ricerche guardando proprio al ruolo del settore privato nel ciberspazio. In particolare, tra i diversi studi, una recente pubblicazione ha mostrato come tali attori, comunemente visti come obiettivi di regolamentazione nel campo della sicurezza delle reti e dell'informazione, siano in grado di influenzare il processo decisionale ed entrare nell'arena diplomatica[40]. Partendo da questa idea, il capitolo ha analizzato le modalità che hanno permesso al settore privato di entrare effettivamente nel processo decisionale, e con quali effetti da un punto di vista legislativo prendendo la proposta normativa della Commissione europea circa la Direttiva Nis come caso di studio.

A tal fine, la prima parte della seguente ricerca si è concentrata sul ruolo del settore privato nella sicurezza delle reti e dell'informazione, partendo dall'idea di globalizzazione e dal processo di *empowerment* degli anni '80, quando i governi di tutto il mondo – per vari motivi – hanno iniziato a collaborare con il settore privato per rispondere ad esigenze di politica pubblica.

La seconda sezione si è focalizzata sullo sviluppo delle politiche eu-

[40] Benjamin Farrand e Helena Carrapico, "Networked Governance and the Regulation of Expression on the Internet: The Blurring of the Role of Public and Private Actors as Content Regulators", in *Journal of Information Technology & Politics*, vol. 10, n. 4 (2013), p. 357-368.

ropee nel campo della cybersecurity con particolare attenzione al ruolo degli attori non-statali. Il 2001 segna l'inizio dell'attività a livello europeo nel campo della protezione delle infrastrutture critiche e in questo stesso anno, la Commissione riconosce che la maggior parte dei servizi critici sono ormai offerti da operatori privati[41]. Dal 2009 in poi, l'Ue propone una serie di iniziative per rafforzare sempre di più la collaborazione tra settore pubblico e privato nel campo della sicurezza informatica. Grazie a queste interazioni ricorrenti – consultazioni pubbliche, gruppi di esperti o altro – sostenute dalla stessa Ue, il caso di studio affrontato nella sezione successiva ha mostrato come attori statali e non-statali hanno creato *policy network*, entrando così nell'arena diplomatica a livello europeo.

La terza sezione, infatti, affronta lo studio delle negoziazioni che hanno portato all'adozione della Direttiva Nis analizzando in concreto il ruolo di operatori di infrastrutture critiche, fornitori di servizi digitali nell'arena politico-decisionale a livello europeo. Questi attori, sulla base di vere e proprie "credenze" hanno formato coalizioni in grado di entrare nella scena diplomatica.

Prima di concludere è possibile fare alcune considerazioni. In primo luogo, il concetto di "responsabilità condivisa" o "sicurezza cooperativa" nel campo della sicurezza delle reti e dell'informazione ha portato all'*empowerment* del settore privato. Tramite questa collaborazione si crea una sorta di interdipendenza tra pubblico e privato, dove entrambe le parti hanno bisogno l'una dell'altra: da un lato, per il settore pubblico lavorare con il settore privato diventa l'unico modo per adempire al proprio ruolo istituzionale e raggiungere necessari obiettivi di politica pubblica – come quello della sicurezza; dall'altro, per il settore privato, collaborare con le istituzioni significa far sentire la propria voce[42].

L'emergere di questi nuovi attori, che gradualmente vengono considerati come essenziali per raggiungere importanti obiettivi di politica pubblica, porta inevitabilmente alla questione della rappresentanza nel processo di identificazione di tali obiettivi. È in questo contesto che si formano coalizioni o *policy network* formati da attori statali e non, basati su credenze e risorse, in grado di influenzare fondamentali decisioni a livello europeo. La Direttiva Nis rappresenta soltanto un esempio da cui si evince abbastanza chiaramente il ruolo di queste coalizioni.

---

[41] Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, cit.

[42] John Peterson, "Decision-making in the European Union", cit.

Con l'emergere di nuovi attori intorno a importanti questioni di politica pubblica, si arriva dunque a un dilemma legato al concetto di rappresentanza: se da un lato gli attori non-statali cominciano ad essere visti come "complementari" per il raggiungimento di importanti obiettivi di politica pubblica, dall'altro emerge la volontà da parte di questi di essere rappresentati, ovvero riconosciuti come attori legittimi con il potere di influenzare lo scorrere degli eventi. È in questo contesto di "crisi della rappresentanza" che attori non-statali si stanno organizzando, più o meno accidentalmente, per entrare a far parte del sistema internazionale. Gradualmente, con lo sviluppo di modelli di rappresentanza sempre più riconoscibili e legittimi, si vedrà – o forse si può già vedere – la nascita di un nuovo sistema diplomatico più "democratico".

Le aziende globali si trovano sempre più spesso ad intervenire a fianco di stati nazionali per risolvere questioni di politica pubblica creando alleanze strategiche con alcuni di questi. Un'indicazione dell'evoluzione del rapporto tra settore pubblico e privato si trova, per esempio, guardando al trattamento riservato agli amministratori delegati delle maggiori società globali i quali vengono trattati quasi come "capi di stato" da parte di governi o di organizzazioni intergovernative. Incontri tra leader del settore privato e alti funzionari statali non sono fuori dall'ordinario e non si limitano a discussioni imprenditoriali o economiche, ma includono scambi di opinione su questioni politiche e sociali.

La diplomazia è una parte necessaria e naturale dell'ordine internazionale, tuttavia non può più essere limitata agli stati nazionali. I ministeri degli Affari esteri non sono più i soli guardiani della diplomazia e devono condividere lo "spazio" diplomatico e imparare a impegnarsi in modo costruttivo con attori non-statali[43]. Forse è arrivato il momento di riconsiderare i tradizionali ruoli della diplomazia pubblica. Guardando avanti, i diplomatici dovranno tenere conto di nuove sfide: allentare le loro abitudini di controllo, adottare diverse mentalità e abbracciare nuove pratiche in un mondo di reti e sfide transnazionali. Il coordinamento strategico di attori statali e non-statali negli sforzi di diplomazia pubblica sarà essenziale in quanto la natura della diplomazia pubblica diventerà solo sempre più complessa, interconnessa e multidirezionale.

[43] Raymond Saner e Lichia Yiu, "International Economic Diplomacy: Mutations in Postmodern Times", cit.

3.
L'accesso ai dati nel cybercrimine transfrontaliero: il regime europeo e l'equilibrio transatlantico

Francesca Bitondo

Sempre più spesso le prove ai fini delle indagini penali si trovano oltre i confini territoriali in cui è esercitata la sovranità statale. Nel mondo digitale e digitalizzato in cui viviamo, anche il crimine non conosce confine e si avvale degli strumenti e dei processi informatici come mezzo per condurre la fattispecie criminosa (dall'invio di una semplice e-mail il cui contenuto include informazioni per l'espletamento del crimine, fino allo sfruttamento di vulnerabilità informatiche stesse). Ad oggi contenuti informatici come post di social network e e-mail sono conservati in Paesi diversi, superando i confini nazionali e connettendo Paesi e persone oltre le delimitazioni geografiche. Si assiste quindi a una conseguente globalizzazione delle prove penali che pone dinanzi a sfide significative per l'applicazione della legge. I tradizionali meccanismi transfrontalieri, come i trattati di mutua assistenza giuridica (Mlat) sono ampiamente considerati troppo lenti e farraginosi e al loro posto diversi Paesi stanno rispondendo con nuovi quadri normativi per gestire ed accedere alle prove elettroniche, con conseguenti effetti sulla privacy e sui diritti umani, oltre a modifiche alle procedure di applicazione della legge e alla più ampia governance di Internet.

Questo capitolo si concentra in particolare sulla proposta del Commissione europea sull'accesso alle prove digitali, comprensiva di un regolamento e di una direttiva, meglio conosciuta come "pacchetto e-Evidence". Successivamente presenta le iniziative intraprese a livello internazionale, dal recente *Clarifying Lawful Overseas Use of Data Act* (Cloud Act) del marzo 2018 degli Stati Uniti sino all'ammodernamento della Convenzio-

ne di Budapest del 2001, per cui gli Stati contraenti stanno lavorando a un protocollo addizionale che disciplini in maniera più specifica l'accesso alle prove digitali.

Pur non potendo prescindere completamente dalla fase descrittiva delle sopracitate iniziative, la trattazione si concentra meno sui dettagli specifici di ciascuna proposta, alla luce sia della natura squisitamente tecnica della materia e sia per la congiuntura temporale (gli effetti non sono ancora noti non essendo questi quadri normativi ancora del tutto definiti). Punta invece a cogliere i tratti geopolitici della tematica: da un lato la globalizzazione del cybercrimine e della prova elettronica e la conseguente esigenza di una cooperazione non solo intergovernativa, ma anche con attori coinvolti in prima linea come i fornitori di servizi digitali, con i riflettori accesi sui diritti umani che ivi si intrecciano; dall'altro la tendenza a volere mantenere i confini geografici nella gestione e nell'accesso al dato in nome di una tutela della sovranità statale.

3.1 L'accesso alle prove elettroniche: attuale funzionamento

Da un punto di vista tecnologico, le autorità di esecuzione sono poste dinanzi a sempre maggiori problemi nell'accedere ai dati nell'ambito di indagini penali internazionali. I dati a cui si fa riferimento sono i dati *at rest*, che includono e-mail, informazioni di social network e una vasta serie di contenuti conservati nel cloud. Per il pubblico ufficiale cui è demandata l'applicazione della legge in Europa e non solo, le prove digitali sono spesso conservate in Paesi diversi dal proprio (spesso negli Stati Uniti) o gestite da un'azienda statunitense. Molto spesso l'ordine di esecuzione o di richiesta di accesso ai dati, o qualsiasi altro mezzo legale usato nel Paese dove il crimine si è consumato, non è sufficiente per potere accedere ai dati archiviati. Stessa logica vale per i dati in transito, come ad esempio per le intercettazioni. Un rapporto della Commissione europea del 2018 ha rilevato che più della metà di tutte le indagini prevedono una richiesta transfrontaliera di accedere a prove elettroniche[1].

[1] Commissione europea, *Commission Staff Working Document Impact Assessment. Accompanying the document Proposal for a Regulation … on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive … laying down harmonised rules on the appointment of legal representatives for the purpose*

"Il carattere di transnazionalità non riguarda soltanto i fenomeni criminali al cui contrasto le autorità degli stati membri sono dedite", ma si propaga altresì nell'"articolazione della rete, vale a dire dell'infrastruttura tramite cui i contenuti sono veicolati o archiviati. Il ricorso sempre più frequente a piattaforme di cloud o a servizi di hosting offerti da operatori" dislocati nel territorio europeo "accresce la probabilità che il luogo di consumazione di una condotta illecita", dove è presente "la giurisdizione dell'autorità procedente, e il luogo di conservazione dei dati che costituiscono prove dell'avvenuta commissione di tale fattispecie criminosa differiscano"[2]. Anche quando tutti altri possibili elementi di un'indagine siano presenti sul territorio di indagine, la localizzazione dei dati o del fornitore di servizi può dare origine a una situazione che supera i confini nazionali. Tuttavia i confini nazionali e la sovranità nazionale restano alla base del nostro sistema giuridico internazionale. In virtù di tale espletamento dei poteri entro i confini di sovranità territoriale, alcuni Paesi stanno perseguendo la soluzione più immediata di acquisizione delle prove digitali, affermando unilateralmente i poteri di polizia al di fuori del proprio territorio. Nondimeno, i mandati di perquisizione criminale che raggiungono le frontiere pongono un problema diverso: essi comportano l'esecuzione di poteri di polizia nel territorio di un altro stato sovrano. Ma tale "giurisdizione esecutiva" potrebbe violare il diritto internazionale e la sovranità di un altro Paese. Per questo è emersa e continua ad affermarsi l'esigenza di introdurre norme *ad hoc* che tengano in considerazione non soltanto l'opportunità di definire misure di carattere speciale rispondenti alle caratteristiche tecniche di Internet e del digitale ma anche l'urgenza di attivare meccanismi di acquisizione di prove in grado di prescindere dalla dinamica fondata sul necessario coinvolgimento delle autorità nazionali, stabilendo dei processi di cooperazione più veloci, efficienti e nel pieno rispetto dei diritti umani. Ad esempio, le autorità competenti dei Paesi dell'Ue si basano su dei mezzi cosiddetti tradizionali di cooperazione giudiziaria o sulla cooperazione volontaria da parte di fornitori di servizi digitali. Per le richieste all'interno dell'Unione normalmente le autorità giudiziarie usano l'Ordine europeo di indagine penale per ottenere

of gathering evidence in criminal proceedings (SWD/2018/118), 17 aprile 2018, p. 14, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52018SC0118.

[2] Oreste Pollicino e Marco Bassini, "La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi", in *MediaLaws*, 26 ottobre 2018, http://www.medialaws.eu/?p=12994.

le prove; per richieste all'esterno, utilizzano i Mlat. Ma proprio perché questi ultimi sono spesso lenti e poco fluidi, le autorità di esecuzione e i fornitori di servizi collaborano su una base volontaria in modo da ottenere le prove digitali in una maniera più celere. Nondimeno, emergono problemi di almeno tre ordini: in primo luogo, la cooperazione pubblico-privato è su base volontaria e spesso questo porta a delle inefficienze nel meccanismo che possono ostacolare le indagini. In secondo luogo, le procedure sono lente: si prenda l'esempio di un attacco terroristico in un Paese A in cui i dati di un messaggio e-mail inviato dal terrorista risiedano in un Paese B. In questo caso il procuratore dello stato A emette la richiesta, previa approvazione del giudice, che deve essere inviata all'autorità centrale/competente dello stato A la quale, a sua volta, inoltra la richiesta all'autorità centrale/competente dello stato B. Tale richiesta viene poi inviata, tramite il giudice dello stato B, al fornitore di servizi, il quale manderà le prove richieste dalle autorità B. Ottenute le prove, lo stato B le invia, quindi, all'autorità centrale dello stato A, il quale le gira al procuratore. Come è possibile intuire, questo processo previsto dai Mlat richiede delle tempistiche non indifferenti per essere completato, con un conseguente ritardo sulle indagini e al cui termine, con molta probabilità, tali prove non saranno neanche più utili ai fini dell'indagine. Ne consegue una mancanza di certezza del diritto: per le autorità giudiziarie poste dinanzi a limiti obiettivi nell'utilizzo di mezzi di indagini transfrontalieri che possono inficiare l'indagine e per gli stessi fornitori di servizi digitali, che si trovano ad operare in un contesto di natura volontaristica e senza precise regole in merito e dovendone rispondere anche ai propri utenti.

Ma qualcosa inizia a muoversi. L'anno 2018 è stato segnato da alcune importanti iniziative legislative negli Stati Uniti e nell'Ue che riflettono un nuovo approccio in materia di accesso alle prove elettroniche da parte dei pubblici ufficiali cui è demandata l'applicazione della legge, al fine di prevedere nuovi strumenti legislativi, o ammodernando quelli esistenti, al fine di consentire la possibilità di richiedere ai fornitori di servizi Internet e cloud di trasferire direttamente i dati richiesti all'autorità che emette tale ordine, e questo indipendentemente dal luogo in cui i dati sono archiviati o dove il sospetto criminale dell'inchiesta risiede. Sia gli Stati Uniti che l'Ue si sono mossi in tal senso. I primi hanno adottato nel marzo 2018 il Cloud Act che, tra l'altro, abilita a negoziare degli accordi bilaterali con altri Paesi per affrontare eventuali conflitti tra la legge statunitense e le leggi di altri stati, seppur applicabili in situazioni limitate.

Poche settimane dopo, il 17 aprile 2018, la Commissione europea ha

proposto un regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale e una direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali[3]. Il regolamento e la relativa direttiva forniscono un quadro che permette alle autorità di polizia degli stati membri di reperire prove elettroniche direttamente dai fornitori di cloud e di altri servizi online a livello transfrontaliero. Il cosiddetto "pacchetto e-Evidence" costituisce l'equivalente europeo della legge Usa e mira, in modo analogo, a definire la cooperazione con i fornitori di servizi e a fornire alle autorità di polizia e giudiziarie strumenti più rapidi per ottenere prove elettroniche.

La tematica, di natura molto tecnica, presenta dei profili problematici per almeno tre ragioni. La prima attiene all'ambito giuridico: i Paesi sono chiamati non solo ad adeguare i propri ordinamenti giuridici e gli strumenti delle autorità di polizia e della magistratura per accedere alle prove digitali di un crimine, ma nel mondo digitale, per sua natura senza confini, gli stati necessitano di lavorare in modo costruttivo per giungere ad accordi internazionali al fine di dare vita a soluzioni transfrontaliere per tutelare i diritti fondamentali e scongiurare il più possibile conflitti legislativi. La seconda ragione riguarda il complesso bilanciamento delle soluzioni da raggiungere tra sicurezza pubblica e diritti fondamentali, quali la privacy, la libertà di espressione, ecc. La terza ragione è prettamente geopolitica: la gestione del dato, in questo caso l'accesso ai dati al fine di ottenere prove elettroniche, è diventato un asset cruciale degli stati, nonché prerogativa, secondo alcuni, dell'esercizio della propria sovranità. Raggiungere delle soluzioni valide e sostenibili è complicato quando sono coinvolti i confini nazionali, in quanto queste soluzioni devono essere perseguite nel quadro del diritto internazionale e della sovranità nazionale.

Comprendere la sfida geopolitica della tematica è essenziale: si tratta di creare un'architettura che se da un lato consente di ammodernare ed efficientare i sistemi di accesso ai dati in un mondo in rapido cambiamento, dall'altro richiede del tempo e uno sforzo da parte dei Paesi, i quali tendono a voler esercitare la propria sovranità sui dati e ad addurre come scusanti ragioni di carattere nazionale che ostacolano accordi internazionali. Inoltre tale esigenza si interfaccia con altri principi fondamentali

[3] Commissione europea, *Proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* (COM/2018/225), 17 aprile 2018, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=COM:2018:225:FIN.

come la tutela della privacy e ne richiede un necessario bilanciamento. Si deve infine tenere conto del ruolo dei fornitori di servizi digitali e dei loro meccanismi di funzionamento.

3.2 La proposta e-Evidence dell'Unione europea

La proposta risponde, come già menzionato, "all'inefficacia degli strumenti finora sperimentati", constatando il "carattere di volatilità delle prove elettroniche, da cui discende la dimensione giocoforza internazionale della relativa disciplina. A livello europeo, in particolare, nessuno degli atti allo stato vigenti contiene un esplicito riferimento alla possibilità per le autorità degli stati membri di accedere presso dati conservati dai fornitori di servizi"[4]. La proposta di Regolamento e-Evidence ha l'obiettivo di inserire uno strumento radicalmente nuovo anziché modificare il quadro esistente, al fine di recepire in maniera più diretta e quanto più efficace i cambiamenti cui ha portato l'era del cloud computing, e più in generale della quarta rivoluzione industriale. In particolare, il pacchetto normativo ambisce a superare una delle principali criticità emerse dall'applicazione degli accordi di reciproca assistenza, legata alle lunghe tempistiche nei processi che coinvolgono le autorità di ciascuno stato membro e che quindi non possono prescindere da una forte centralizzazione.

Per tale ragione, la Commissione europea ha introdotto una serie di strumenti standard per l'acquisizione di prove, l'ordine europeo di produzione (Epo) e l'ordine europeo di conservazione (Epro), al fine di evitare il dispendio di tempo e risorse necessari ad attuare forme di cooperazione che inevitabilmente seguono iter diversi per ciascuno dei Paesi interessati. Tali strumenti rispondono quindi all'esigenza di avere una procedura unica e quanto più armonizzata per i Paesi membri che, decisa quindi a monte, potrebbe accelerare le indagini. Soprattutto, nella proposta dell'Unione un riferimento importante è il rispetto dei diritti umani fondamentali che vengono messi senz'altro in rilievo nella misura in cui sia necessario accedere a dati conservati presso un operatore terzo e formare le relative prove elettroniche, aspetto non tenuto in conto dagli

[4] Oreste Pollicino e Marco Bassini, "La proposta di Regolamento e-Evidence…", cit. Vedi anche Tommaso De Zan e Simona Autolitano (a cura di), "EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace", in *Documenti IAI*, n. 16|17 (novembre 2016), https://www.iai.it/it/node/7049.

accordi di mutua assistenza. Questo rappresenta un elemento di novità, certamente non nuovo alla storia e all'approccio dell'Ue, ed evidenzia il fatto cruciale che ogni "misura direttamente o indirettamente in correlazione con l'accesso a dati in formato digitale si pone in naturale tensione" con una serie di diritti non circoscritti "alla sola privacy e alla tutela dell'identità personale", ma anche ad altri quali la libertà di pensiero[5]. Questo delicato bilanciamento ha, inoltre, una portata internazionale e rappresenta quindi un ulteriore elemento di complicazione, laddove si pensi come su questi diritti si possano esercitare sensibilità e visioni diverse, incardinate nei rispettivi ordini costituzionali. Ad esempio, gli Stati Uniti potrebbero manifestare una maggiore inclinazione a favorire l'esercizio della libertà di parola rispetto ai Paesi europei, i quali a loro volta, hanno una visione maggiormente protettiva della privacy e dei dati personali, come dimostrato dal Gdpr. La necessità di un atto che codificasse nuovi strumenti adatti al contesto tecnologico con cui devono interagire era dunque cogente e la proposta di regolamento e-Evidence recepisce queste istanze, cercando di fare in modo che la tutela dei diritti fondamentali costituisca la cartina al tornasole per l'efficace funzionamento dei meccanismi contemplati.

Quanto ai contenuti cardine della proposta, di seguito ne sono elencati alcuni che hanno particolare rilevanza nel definire la nuova architettura normativa e procedurale. Si è detto come il pacchetto proposto intende offrire una risposta al problema della volatilità e della conseguente dimensione transnazionale delle prove elettroniche. "La proposta istituisce infatti un comune meccanismo di formazione delle prove in ambito digitale" a disposizione delle autorità degli stati membri. Gli strumenti individuati a tale scopo sono due: da un lato l'Epo, dall'altro lato l'Epro, diretti ad ottenere rispettivamente "l'acquisizione ovvero la conservazione di dati in previsione della relativa produzione come prove nell'ambito di un'indagine o di un processo penale in corso nel Paese di emissione"[6]. Concretamente, gli ordini di produzione e conservazione sono adottati dalle autorità dello stato di emissione e sono rivolti direttamente e senza intermediazione ai fornitori di servizi, nella figura del rispettivo rappresentante legale designato per uno stato membro[7]. È subito possibile co-

[5] Barbara Calderini, "Cloud act, la norma USA che fa a pugni con la privacy europea: i nodi", in *Agenda digitale*, 11 giugno 2019, https://www.agendadigitale.eu/?p=65910.

[6] Oreste Pollicino e Marco Bassini, "La proposta di Regolamento e-Evidence…", cit.

[7] Ibid.

gliere, anche alla luce del funzionamento attuale del meccanismo sopra menzionato, l'elemento di novità: non più la "necessaria interlocuzione tra le autorità dello stato di emissione e dello stato di esecuzione" ma la disintermediazione di questa[8], in quanto l'autorità dello stato di emissione di un ordine di produzione o conservazione manda la richiesta direttamente al prestatore di servizi per ottenere dati rilevanti ai fini del procedimento penale.

I fornitori di servizi digitali dovranno quindi designare un rappresentante legale come previsto dalla direttiva che accompagna il regolamento e-Evidence, in assenza di tale designazione gli ordini saranno rivolti a qualsiasi stabilimento del prestatore di servizi nell'Unione. È importante sottolineare la portata dell'ingresso nell'architettura disegnata dalla Commissione degli attori privati, i quali diventano un vero e proprio meccanismo che funge da valvola di sfogo in tale procedimento, dovendo assicurarsi che gli ordini ricevuti non presentino vizi o errori di fatto e che costituiscano la base per permettere di sollevare una possibile obiezione. Ma, più in generale, questo meccanismo denota un trend fondamentale, ossia una collaborazione sempre più estesa e sempre più intensa tra attori pubblici e privati nel campo del digitale, in quanto, in molte delle sue espressioni, gli attori privati del digitale rivestono un ruolo preponderante. Un altro aspetto fondamentale riguardo tali strumenti sarà evitare i tentativi di elusione. Infatti oggi alcuni stati membri richiedono i dati direttamente presso i fornitori di servizi anche quando tali dati sono conservati o controllati da un soggetto in un altro stato membro. Per assicurare che gli stati membri non aggirino il ricorso agli Epo e le tutele da questi previste, il regolamento dovrebbe imporre agli stati membri l'utilizzo degli Epo e delle altre procedure previste dal diritto dell'Unione quando tali procedure sono applicabili. In tutti gli altri casi, prima di ricorrere ai meccanismi disponibili ai sensi della legislazione nazionale, gli stati membri dovrebbero affidarsi all'assistenza giuridica reciproca al fine di ottenere i dati, soprattutto tenendo conto del fatto che l'approccio unilaterale ed elusivo degli strumenti standard non garantisce lo stesso stato di diritto e le stesse garanzie dei diritti umani previste dal regolamento.

L'articolo 1 della proposta di regolamento prevede una classificazione per categoria dei tipi di dati che ricadono nell'ambito di applicazione del regolamento stesso (dati relativi agli abbonati, dati relativi agli accessi, contenuti e dati relativi alle operazioni). In tutti i casi, il regolamen-

[8] Ibid.

to prescrive che gli Epo emessi per detti dati debbano essere necessari e proporzionati. Ad ogni modo, nel caso dei dati ritenuti maggiormente sensibili (come i contenuti o i dati relativi alle operazioni), si applicano garanzie supplementari. Ad esempio, gli Epo per i contenuti utente e i dati relativi alle operazioni devono essere emanati o convalidati da un organo giurisdizionale o da un giudice e possono essere adoperati solo nella ricerca di prove relative a un reato grave.

Sono altresì fissati dei limiti temporali abbastanza stringenti entro i quali i fornitori di servizi sono tenuti a fornire le prove richieste: 10 giorni come regola generale e 6 ore nei casi urgenti. Tale aspetto ha già sollevato non poche critiche in fase di negoziato, in quanto non consentirebbe ai fornitori di servizi la possibilità di effettuare i dovuti accertamenti sull'ordine, nonché la corretta composizione delle prove richieste. Inoltre, ai fini della presente analisi, è opportuno fare riferimento agli articoli 15 e 16 che cercano di gestire una tematica complessa, ossia i conflitti tra legislazioni straniere: data la natura transfrontaliera delle comunicazioni elettroniche e dell'e-commerce, talvolta le richieste di dati utente avanzate dalle autorità di polizia degli Stati membri fanno scattare disposizioni di legislazioni straniere che ne proibiscono la divulgazione (come la legge statunitense sulla privacy delle comunicazioni elettroniche). È importante rilevare che il regolamento Ue, agli articoli 15 e 16, stabilisce meccanismi in base ai quali gli organi giurisdizionali possono revocare gli Epo in caso di violazione del diritto di un Paese terzo, soprattutto nel caso di leggi volte a proteggere i diritti e gli interessi fondamentali. Ai sensi della proposta, nel caso in cui un prestatore opponga un'obiezione sulla base di un conflitto con una legge straniera a tutela dei diritti e degli interessi fondamentali, il quesito deve essere sottoposto a un organo giurisdizionale dello stato membro. Laddove l'organo giurisdizionale riscontri un conflitto, esso dovrà chiedere all'autorità estera di indicare la propria obiezione e, nel caso in cui questa non risponda entro la scadenza stabilita, l'organo giurisdizionale dello stato membro confermerà l'ordine. Per quanto si tratti di un buon punto di partenza, il meccanismo sta sollevando diversi quesiti, attualmente in fase di discussione, in sede istituzionale europea, tra cui la richiesta alle autorità estere di rispondere a un organo giurisdizionale di uno stato membro entro 15 giorni (prevedendo un breve periodo di proroga), un lasso di tempo che per alcuni governi potrebbe risultare impraticabile.

Per riassumere, la proposta del pacchetto e-Evidence rappresenta un passo in avanti nell'ammodernamento degli strumenti per attingere alle

prove elettroniche nell'era del cloud computing. Sebbene il tema sia complicato per alcune delle ragioni summenzionate, è altresì vero che un'armonizzazione delle procedure condurrà a indagini più efficienti, veloci e al passo con il progresso tecnologico. Inoltre, un approccio organico interno dell'Ue faciliterà probabilmente il suo ruolo in due negoziati, la cui apertura è stata recentemente autorizzata da parte del Consiglio, che si espleteranno nei prossimi mesi e che avranno un'importanza cruciale: il negoziato con gli Stati Uniti sotto il Cloud Act e il negoziato per il secondo protocollo addizionale della Convenzione di Budapest[9]. L'apertura di questi due tavoli si scontra tuttavia con l'attuale periodo di transizione del nuovo mandato delle istituzioni Ue a seguito delle elezioni europee tenutesi nel maggio 2019 e con un processo al momento fermo all'analisi del Parlamento europeo e non ancora in fase di trilogo (il negoziato tra Commissione, Consiglio e Parlamento per raggiungere l'approvazione del testo e la conclusione dell'iter legislativo). Una fase importante, quindi, sia per l'avanzamento normativo, sia per il ruolo che l'Ue dovrà giocare a livello transatlantico e internazionale.

3.3 Equilibrio internazionale: accordo transatlantico e Convenzione di Budapest

Il Cloud Act, approvato dal Congresso nel marzo 2018[10], ha segnato un passo fondamentale nel quadro normativo statunitense e nell'approccio all'accesso transfrontaliero alle prove, sostituendo il precedente – e anacronistico – Stored Communications Act del 1996 sulla riservatezza delle informazioni conservate dai fornitori di tecnologia. Il tema negli Stati Uniti è stato all'attenzione di *policymaker* ed esperti giuridici anche per il noto "Warrant Case", meglio conosciuto in Europa come "Irish case" (caso Irlanda), risalente al dicembre del 2013, a seguito del rifiuto di Microsoft di fornire dei dati di un'e-mail immagazzinati a Dublino, in Irlanda. Brevemente, la richiesta si inseriva nell'ambito di un'inchiesta condotta dagli Stati Uniti. In particolare, a seguito della richiesta del governo statuniten-

[9] Commissione europea, *Unione della sicurezza: la Commissione riceve il mandato per negoziare norme internazionali sull'ottenimento delle prove elettroniche*, 6 giugno 2019, https://europa.eu/rapid/press-release_IP-19-2891_it.htm.

[10] H.R. 4943 - 115th Congress: Cloud Act, 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943.

se, una corte federale aveva rilasciato l'autorizzazione per il mandato di perquisizione, sulla base delle disposizioni contenute nello Stored Communications Act. Microsoft aveva sostenuto che la legge sulle comunicazioni a cui il governo faceva riferimento non conferiva in alcun modo alle autorità statunitensi il potere di interferire oltre i confini giuridici nazionali e di accedere alle e-mail poste sotto giurisdizione extraterritoriale. Gli Stati Uniti, di contro, ritenevano che Microsoft potesse accedere ai dati dagli Stati Uniti e quindi il luogo in cui i dati erano verificati non importasse. Il Cloud Act è quindi intervenuto a sanare un *vacuum* nel quadro normativo statunitense, ponendo non solo termine al caso emblematico di Microsoft, ma aprendo altresì la strada a meccanismi di negoziato bilaterali per gestire l'accesso transfrontaliero ai dati.

Il Cloud Act crea quindi le basi per una nuova generazione di accordi internazionali, preservando i diritti dei fornitori di servizi cloud di proteggere i diritti alla privacy fino a quando tali accordi non saranno in vigore. Inoltre, la nuova legge stabilisce un meccanismo per gli altri Paesi per accedere al contenuto delle comunicazioni detenute dai fornitori di servizi statunitensi. Ai sensi della legge sulla privacy delle comunicazioni elettroniche (Electronic Communications Privacy Act, Ecpa), alle società statunitensi è vietato divulgare direttamente i contenuti delle comunicazioni ai governi stranieri. I governi stranieri sono invece tenuti a predisporre un trattato (Mlat) o altri tipi di richieste diplomatiche per accedere ai dati, anche quando sono i dati dei loro cittadini in relazione a fattispecie o eventi criminosi locali. Questo è stato in passato un motivo di frustrazione per molti governi, in particolare dal momento che la maggior parte dei dati basati nel cloud sono detenuti da fornitori di servizi digitali statunitensi.

Il Cloud Act consente di superare queste restrizioni in determinate circostanze, sulla base dell'adozione di "accordi esecutivi" tra gli Stati Uniti e altri Paesi, soggetti a una serie di requisiti sostanziali e procedurali di base. Quando sono in atto accordi esecutivi, le disposizioni di blocco dell'Ecpa sono parzialmente revocate e i Paesi possono richiedere direttamente il contenuto delle comunicazioni dei cittadini non residenti negli Stati Uniti e dei loro cittadini ai fornitori di servizi. Il Cloud Act autorizza questi accordi esecutivi solo per i Paesi che soddisfino i requisiti in materia di diritti umani e stato di diritto, assieme a una corposa lista di caratteristiche per ogni richiesta. Alcuni giuristi sostengono che questa tipologia di accordi possano, oculatamente formulati, contribuire a incrementare i livelli di privacy e protezione dei diritti umani. Sono tuttavia state avan-

zate altrettante critiche su un livello di protezione troppo stringente[11]. Il primo di questi accordi esecutivi, i cui negoziati sono stati aperti già nel 2016 e tuttora in corso sotto il nuovo Cloud Act, è quello con il Regno Unito. Inoltre, come su menzionato, lo scorso 6 giugno il Consiglio ha dato mandato ufficiale alla Commissione europea come negoziatore unico con gli Stati Uniti sull'accordo esecutivo. Se l'Ue deve fare i conti con un contesto interno disomogeneo in termini di leggi penali nazionali per avere organicità normativa e non è stata esente da critiche per il conferimento del mandato a negoziare[12], gli Stati Uniti non hanno esitato a esprimere la propria preferenza per fasci di accordi bilaterali, sul modello Regno Unito. I prossimi mesi saranno cruciali per la gestione della tematica e per le relative iniziative.

Anche conosciuta come "Convenzione sul crimine informatico", la Convenzione di Budapest è il principale trattato internazionale incentrato sul cybercrimine, adottata dal Consiglio d'Europa (con la partecipazione attiva di stati osservatori come Canada, Filippine, Giappone, Stati Uniti, Sud Africa) nel 2001 e entrata in vigore nel 2004, con ratifica aperta a tutti gli stati anche non facenti parte del Consiglio d'Europa[13]. Gli Stati Uniti, ad esempio, hanno aderito nel 2006, mentre manca la Russia che ha sempre attribuito alla Convenzione delle forme di ingerenza nella sicurezza nazionale. L'Italia ha invece aderito nel 2008[14]. La Convenzione è il primo trattato internazionale sulle infrazioni penali commesse via Internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete[15]. Contiene inoltre una serie di misure e procedure, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro il cyber-

[11] Jennifer Daskal e Peter Swire, "Privacy and Civil Liberties Under the CLOUD Act: A Response", in *Lawfare*, 21 marzo 2018, https://www.lawfareblog.com/node/14814.

[12] Chloé Berthélémy, "EU Rushes Into E-Evidence Negotiations Without Common Position", in *EDRi*, 19 giugno 2019, https://edri.org/?p=21198.

[13] Consiglio d'Europa, *Dettagli del Trattato n°185*, https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/185.

[14] Consiglio d'Europa, *Stato delle firme e ratifiche di trattato 185*, https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/185/signatures.

[15] Consiglio d'Europa, *Convenzione sulla criminalità informatica*, Budapest, 23 novembre 2001, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f423d.

crimine, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale. Le misure di acquisizione dei dati informatici si incentrano, da un lato, su disposizioni in tema di raccolta in tempo reale di dati sul traffico e relativi al contenuto delle comunicazioni (intercettazioni), dall'altro sulla necessità che gli ordinamenti interni adottino misure legislative per consentire alle proprie autorità l'accesso, la perquisizione ed il sequestro di dati informatici, incluso il potere di fare e trattenere copie degli stessi mantenendo l'integrità dei dati originari. Inoltre, tende ad armonizzare le fattispecie di reato riguardanti la criminalità informatica, a dotare i Paesi firmatari della Convenzione degli strumenti necessari allo svolgimento delle indagini e al perseguimento dei crimini correlati all'area informatica e a costruire, infine, un efficace regime di cooperazione internazionale. La Convenzione estende la portata del reato informatico includendo tutti i reati in qualunque modo commessi mediante un sistema informatico, anche nel caso in cui la prova del reato sia sotto forma elettronica. Inoltre, stabilisce tre principi generali nella cooperazione internazionale: (a) deve essere perseguita nella misura più ampia possibile; (b) deve essere estesa a tutti i reati relativi ai sistemi e ai dati informatizzati; (c) deve rispettare non soltanto le disposizioni della Convenzione, ma anche essere conforme agli accordi internazionali in materia. La Convenzione è articolata in quattro capitoli: definizioni, misure da adottare a livello nazionale in tema di diritto sostanziale e processuale, cooperazione internazionale, clausole finali. In particolare, la Convenzione prevede un certo numero di misure normative di diritto penale sostanziale che le parti devono adottare a livello nazionale. Cerca altresì di combattere, tra l'altro, l'accesso illegale, intenzionale e senza diritto a tutto o a parte di un sistema informatico; le intercettazioni illegali e cioè delle intercettazioni di dati informatici, intenzionali e illecite, effettuate attraverso mezzi tecnici durante trasmissioni non pubbliche; dell'attentato all'integrità dei dati (danneggiamento, cancellazione, deterioramento, alterazione e soppressione dei dati informatici) fatto intenzionalmente e senza autorizzazione; l'attentato all'integrità dei sistemi, concretantesi in un impedimento grave al funzionamento di un sistema informatico, effettuato intenzionalmente e senza diritto mediante il danneggiamento, la cancellazione il deterioramento, l'alterazione e la soppressione dei dati informatici.

Nel settembre 2017 il Consiglio d'Europa ha aperto i negoziati per il Secondo Protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica. L'obiettivo del protocollo è quello di stabilire disposizioni

per un regime di assistenza legale reciproca più efficace e semplificato, favorendo la cooperazione diretta tra stati parti della Convenzione e i fornitori di servizi e di estendere le ricerche oltre i propri confini territoriali nazionali. Il vantaggio di tale accordo è il suo potenziale di applicazione in buona parte del mondo, poiché già attualmente, 63 Paesi fanno parte della Convenzione. I negoziati sono iniziati nel 2017 e termineranno il 2019. Sebbene le discussioni siano ancora in corso, sappiamo che queste si concentrano su quattro aree principali: (1) cooperazione internazionale intergovernativa; (2) cooperazione tra i governi e i fornitori di servizi digitali; (3) standard per l'accesso e la sicurezza; (4) più in generale, requisiti per la protezione dei dati. Gli Stati Uniti, impegnati nei negoziati, saranno in prima linea con il limite di non avere delle fattispecie criminose nella legge interna e l'opportunità, parallelamente al processo di cooperazione internazionale, di ammodernare le leggi interne.

Sull'equilibrio internazionale in costruzione in termini di accesso legale ai dati vale la pena menzionare altre due importanti sfide, la cui trattazione andrebbe oltre i limiti del presente elaborato: innanzitutto il modo in cui si stanno muovendo altri attori preponderanti nello scacchiere globale. Sebbene a livello transatlantico delle iniziative vengono certamente portate avanti sia in quadri internazionali che interni e bilaterali, con le dovute necessità e difficoltà di concertazione, se definiamo l'accesso ai dati per il loro carattere transfrontaliero e interconnesso, è opportuno interrogarsi come altri attori di rilievo a livello globale e digitale come la Cina intendano gestire la tematica. Ad esempio la Russia e la Cina, tra gli altri[16], hanno promulgato leggi che richiedono la "localizzazione dei dati", ovvero la conservazione dei dati comunicazione all'interno del Paese. La localizzazione dei dati consentirebbe di conservare i dati nel Paese, soggetti alle norme nazionali per l'accesso a questi (o alla mancanza di regole) La seconda sfida attiene poi all'utilizzo crescente, anche nel campo penale e da parte delle autorità di polizia, come rilevato da un recente rapporto dell'Interpol e dell'Istituto interregionale delle Nazioni Unite per la ricerca sul crimine e la giustizia (Unicri)[17], di sistemi di intelligenza artificiale e *machine learning*, ossia la scienza che programma i computer in modo da imparare dai dati. I modelli di *machine learning* sono sempre

[16] Information Technology Industry Council, *Data Localization Snapshot Current as of January 19, 2017*, https://www.itic.org/policy/forced-localization/data-localization.

[17] Interpol e Unicri, *Artificial Intelligence and Robotics for Law Enforcement*, 21 marzo 2019, http://www.unicri.it/news/article/Artificial_Intelligence_Robotics_Report.

più usati nella vita quotidiana, dal campo automobilistico a quello della diagnostica sanitaria e del commercio finanziario. Da una prospettiva penale, il punto principale è che questi modelli prendono delle decisioni sulla base di input ricevuti dai dati. Se il modello viene alimentato da set di dati viziati, intenzionalmente o meno, è una questione che avrà sempre più rilevanza in futuro e avrà certamente risvolti nel campo giuridico, che attualmente non prende in considerazione tale responsabilità, nonché l'intenzione a monte.

Conclusioni: sovranità dei dati o cooperazione globale?

Dal monopolio dell'uso della forza al monopolio del dato, la tendenza ad applicare la sovranità al campo digitale è una prerogativa che molti stati, in diversi settori, stanno avanzando. Mentre iniziative normative come il pacchetto e-Evidence sono in fase di sviluppo, altri Paesi si stanno muovendo su binari diversi con un approccio alla localizzazione del dato. Nondimeno, questo tipo di leggi può avere anche dei notevoli effetti negativi. Le norme sulla localizzazione dei dati possono essere una minaccia alla privacy e ai diritti umani, aiutando alcuni regimi repressivi ad accedere ai dati senza le protezioni di base sulla privacy e i diritti fondamentali in vigore. La localizzazione minaccia quindi un beneficio fondamentale di Internet, che ha permesso, ad esempio, ad attivisti per i diritti umani di utilizzare i servizi Internet globali che si trovano al di fuori della giurisdizione territoriale della loro nazione, pur essendo protetti da forme di sorveglianza nazionale. Oltre al quadro normativo della Convenzione di Budapest entro il quale si stanno muovendo gli stati per avanzare sulla tematica, altre iniziative stanno emergendo: ad esempio l'Australia sta valutando una riforma in materia. La Canadian Association of Chief of Police ha recentemente approvato una risoluzione per aprire ai negoziati con gli Stati Uniti sotto l'egida del Cloud Act. Ancora, in India è in corso un dibattito sui requisiti della localizzazione dei dati affinché si delinei un accesso legale a questi.

Temi come l'accesso alle prove elettroniche richiedono necessariamente degli accordi seri e sostenibili che siano a beneficio della società, sia nel rispetto del progresso tecnologico, sia nell'interesse dei cittadini e dello stato ad avere processi efficienti e più rapidi. Per combattere il crimine e proteggere la sicurezza pubblica, i governi devono assolutamente poter accedere ai dati digitali secondo procedure e processi normati dal-

la legge. Lo sviluppo di leggi moderne che forniscano alle autorità giudiziarie e di sicurezza nazionale meccanismi appropriati per accedere ai dati digitali in seguito a processi legali ben definiti e concordati è una priorità fondamentale. Poiché la maggior parte delle leggi delle singole nazioni non è stata al passo con le tecnologie, oggi quando i dati vengono spostati nel cloud sorgono dei dubbi relativamente ai sistemi giudiziari che governano l'accesso ai dati archiviati. Inoltre, la mancanza di sistemi internazionali di accesso alle prove digitali fa sì che i governi adottino sempre di più misure unilaterali per acquisire i dati memorizzati all'esterno dei propri confini. Ciò può comportare conflitti giurisdizionali di notevole complessità che potrebbero indebolire le leggi oppure obbligare le aziende a dover scegliere di non rispettare le leggi di una nazione per osservare quella di un'altra.

Una corretta gestione del ciberspazio passa anche dalla garanzia che i crimini commessi nel o tramite il ciberspazio non sfuggano al *law enforcement*. È quindi fondamentale che esista un'architettura solida che garantisca certezza del diritto e una fluida collaborazione tra autorità giudiziali, autorità di polizia e fornitori di servizi digitali. Modernizzare le norme è possibile solo trovando il giusto equilibro fra una serie di diritti fondamentali (come il diritto alla privacy, alla libertà di parola e alla sicurezza pubblica) e cercando di garantire trasparenza e un processo legale chiaro e puntuale. Sebbene di non facile attuazione per la diversità di leggi nazionali e la peculiarità della materia, in cui la sicurezza pubblica gioca un ruolo fondamentale, è nondimeno necessario potere avanzare ai fini della certezza del diritto e nella gestione di una tematica sempre più cruciale a livello internazionale.

PARTE II
LA GEOPOLITICA DEL DIGITALE: PROSPETTIVE E SFIDE GLOBALI

4.
Tra bombe atomiche e armi cibernetiche: teoria e governance delle minacce nucleari all'epoca del ciberspazio

Roberta Mulas

Fin dai tempi di WarGames, il film del 1983 in cui un giovane hacker americano riesce a fare breccia nei sistemi per il lancio dei missili rischiando di scatenare una guerra nucleare tra Usa e Urss, il legame tra la bomba atomica e l'informatica cattura con potenza l'immaginario collettivo. Ma non è solo la commistione di due tecnologie dalle enormi potenzialità distruttive a dover far riflettere. La rivoluzione cibernetica, come quella nucleare prima di lei, ha creato un nuovo tipo di tecnologia militare portando con sé l'esigenza di ridefinire il paradigma della sicurezza. Più interessanti degli scenari apocalittici di azioni cibernetiche che interferiscono coi sistemi di comando e controllo delle testate nucleari, è il modo in cui questa nuova tecnologia funziona nel contesto della politica di sicurezza di uno Stato.

Questo capitolo propone una preliminare riflessione sull'esperienza maturata in ambito nucleare, applicandola all'attuale contesto di crescente digitalizzazione in ogni area delle relazioni umane, inclusa quella cruciale dei conflitti internazionali. L'avvento del digitale ha infatti riprodotto alcune delle dinamiche osservate con l'inizio dello sfruttamento dell'atomo, tanto per scopi bellici che civili. In entrambi i casi si tratta di una tecnologia che promette a chi la possiede grandi vantaggi economici, ma anche la capacità di infliggere perdite sostanziali se usata in maniera offensiva. Ha quindi senso "ripassare" quel che ci hanno insegnato le armi nucleari riguardo all'applicazione bellica di una nuova tecnologia e alla sua governance internazionale.

Il parallelo con la rivoluzione nucleare permetterà di investigare l'utilità di concetti sviluppati durante gli oltre 70 anni di storia della bomba per l'attuale contesto della cybersecurity. In primo luogo, si rifletterà su quali azioni intraprese nel ciberspazio possano essere considerate alla stregua di un attacco armato e dunque come le armi cibernetiche possano essere impiegate in maniera coercitiva, esaminando la rilevanza della dottrina della deterrenza nucleare. L'applicazione della forza o la sua minaccia, tuttavia, non sono gli unici modi in cui si sono strutturate le relazioni tra stati all'ombra dell'atomica. Si proseguirà quindi con un'analisi degli strumenti internazionali di non-proliferazione e controllo degli armamenti con i quali è stata introdotta una certa moderazione e prevedibilità nelle relazioni nucleari. Per concludere si richiamerà un ulteriore elemento legato all'evoluzione della governance delle armi nucleari, ovvero l'importante ruolo svolto, fin dal principio, dagli scienziati nel richiamare a un utilizzo responsabile della tecnologia da loro creata.

4.1 La tecnologia come arma

La rivoluzione digitale ha modificato profondamente tutta una serie di ambiti della vita, dalle comunicazioni personali alla produzione industriale, dalla creazione del consenso politico alle transazioni finanziarie. Quel che interessa questo capitolo è la dimensione bellica, e dunque come cyber e nucleare entrino a far parte della "cassetta degli attrezzi" strategica nazionale e influiscano così sugli equilibri globali. Se in ambito atomico gli usi bellici sono risultati evidenti – e prioritari – fin da principio, vale la pena chiedersi quali siano i confini della dimensione bellica del ciberspazio e se si possa parlare di armi cibernetiche. D'altronde un attacco cibernetico, per quanto noto, non ha ancora mietuto vittime né tantomeno vi è stata una guerra cibernetica, con scambio di colpi tra avversari che terrorizzassero popolazioni e creassero danni irreparabili. Secondo Thomas Rid "non ci sarà una guerra cyber" dal momento che sabotaggio, spionaggio e sovversione sono gli scopi prevalenti degli attacchi cibernetici di matrice politica[1].

Ciononostante, processori e reti hanno il potenziale di innescare distruzioni su larga scala e anche di causare perdite umane. Il caso Stuxnet è forse l'esempio migliore di come strumenti cibernetici possano fungere

[1] Thomas Rid, *Cyber War Will Not Take Place*, Oxford, Oxford University Press, 2013.

da vettore per infliggere perdite materiali a un avversario, sfruttando gli effetti cinetici provocati da un hack. Nel caso in esame vi fu un sabotaggio tramite malware dei sistemi di controllo delle centrifughe nell'impianto iraniano per l'arricchimento dell'uranio di Natanz. L'intrusione consentì agli hacker di modificare la programmazione delle centrifughe che, ormai non più controllate dagli scienziati dell'impianto, iniziarono a girare più velocemente del normale fino a rompersi a causa delle vibrazioni. Si stima che circa un migliaio di centrifughe siano state così distrutte nel 2010 e, anche se non vi furono perdite umane, i danni sarebbero stati tali da rallentare di mesi i progressi nucleari dell'Iran.

Provocare reazioni cinetiche tramite attacchi informatici è dunque possibile, in particolare – come per Stuxnet – attraverso i moderni sistemi di controllo industriale, quali gli Scada, usati in una molteplicità di applicazioni industriali. Ma la crescente digitalizzazione di oggetti fisici – dai frigoriferi agli impianti di riscaldamento e, in un futuro non troppo lontano, le macchine senza guidatore, gli impianti medici e le smart city – indica che vi sono sempre più punti esposti a un possibile attacco cibernetico dalle conseguenze materiali. Le installazioni per l'arricchimento dell'uranio sono solo una delle infrastrutture critiche che in misura sempre maggiore dipendono da processori e reti per la propria operatività – e sono dunque potenziali vittime di attacco informatico. Si può quindi immaginare quali sarebbero gli effetti di un attacco che crei un'esplosione in un reattore nucleare, o un'interruzione delle linee elettriche, dei sistemi di controllo dei cieli, delle reti di telecomunicazione o degli impianti che gestiscono una diga. Non solo tali attacchi potrebbero causare danni ingenti, ma anche mietere un altissimo numero di vittime.

Già nel 2012 l'allora segretario della Difesa americano Leon Panetta aveva messo in guardia da una "Pearl Harbor cibernetica", cioè quanto avverrebbe nel caso in cui un aggressore attaccasse le infrastrutture critiche del Paese, un attacco che sarebbe ancor più distruttivo se messo in atto congiuntamente con uno fisico. Lo stesso anno l'ufficio legale del Dipartimento di Stato americano aveva fatto sapere che un attacco cibernetico dalle conseguenze comparabili a un attacco armato avrebbe potuto innescare l'appello al diritto all'autodifesa ai sensi dell'articolo 51 della Carta delle Nazioni Unite. Benché tale posizione non sia condivisa unanimemente a livello multilaterale[2], è indubbio che si stia procedendo

[2] Nel 2017 il Group of Governmental Experts (Gge) dell'Onu, un consesso di esperti di nomina statale che ha il compito di definire le regole che dovrebbero guidare l'attività

nel senso di una militarizzazione del ciberspazio, di matrice sia difensiva che offensiva. Sono sempre più numerosi gli stati dotati di un comando operativo cibernetico, ovvero che hanno dotato le proprie forze armate di una capacità cyber offensiva, benché si sappia poco di quel che fanno gli eserciti di hacker di Stato. Anche l'Italia dal 2017 sta sviluppando le proprie forze armate cyber – il Comando interforze Operazioni cibernetiche – sotto la guida del generale Francesco Vestito.

Quindi il ciberspazio può esser manipolato per uccidere e ciò sta entrando sempre più nel calcolo strategico degli stati influenzandone la politica militare. A questo riguardo è opportuno puntualizzare le principali somiglianze e differenze tra le due tecnologie in esame: su tutte il grado di difendibilità, da un lato, e la scala distruttiva e l'attribuzione dell'attacco, dall'altro. Proprio come nel caso delle armi nucleari, anche gli strumenti informatici hanno un'eccezionale capacità di penetrare le difese. In campo nucleare i tentativi di sviluppare sistemi di difesa anti-missilistica, in grado di intercettare una testata atomica in arrivo, rimangono ancora oggi lontani dalla perfezione, mentre per quanto riguarda il ciberspazio è virtualmente impossibile mettere in campo difese in grado di resistere a una minaccia in continua evoluzione. Ciò non implica che sia inutile predisporre sistemi difensivi, ma costringe a fare i conti con una situazione di vulnerabilità latente per ogni dispositivo collegato a Internet e, seppur in misura minore, per ogni oggetto che incorpori del codice informatico.

La più lampante differenza riguarda gli impatti di un possibile attacco: gli ordigni atomici si basano sull'innesco di una reazione a catena che produce un'esplosione molte volte più potente rispetto a quanto possibile con testate convenzionali. La bomba lanciata su Hiroshima aveva una potenza equivalente a circa 15.000 tonnellate di tritolo (Tnt) mentre quella più potente mai testata, la Tsar Bomba sovietica, supera i 200 milioni di tonnellate di Tnt. Gli effetti distruttivi su larga scala causati dalla palla di fuoco e dall'onda d'aria e di calore che derivano da una simile esplosione – e le durature ricadute su popolazioni e ambiente conseguenza delle radiazioni – sono difficilmente raggiungibili con strumenti digitali. È pur vero, tuttavia, che il ciberspazio può esser manipolato per infliggere attacchi distruttivi e potenzialmente letali causando danni massicci, dura-

degli stati nel ciberspazio, non riuscì a concordare un rapporto unanime proprio a causa delle divergenze su questo punto: gli Usa insistevano affinché il documento legittimasse il diritto all'autodifesa e l'applicazione del diritto umanitario internazionale al ciberspazio, nozioni contestate da Russia, Cina e Cuba.

turi ed estesi sul territorio – a volte ben più diffusi di quelli di una singola arma nucleare.

Se è ben chiaro cosa sia una bomba atomica, assai meno incontrovertibile è cosa costituisca un'arma cibernetica. Nel 2016 il segretario alla Difesa americano, Ashton Carter, riferendosi alle azioni di contrasto a Daesh affermò che gli Stati Uniti lanciavano "bombe cibernetiche", oltre a quelle convenzionali. Si ritiene che per poter parlare di arma cyber siano necessari almeno tre requisiti: un metodo di propagazione, cioè il modo in cui un malware arriva all'interno della rete da attaccare (che sia un'e-mail di *phishing* o una chiavetta Usb infetta); un exploit, ovvero una porzione di codice progettata per compromettere il software in modo da garantire a una terza parte di effettuare operazioni; e infine un *payload*, cioè il "carico esplosivo" del malware che attacca il sistema[3].

L'attribuzione è la seconda evidente differenza tra attacchi nucleari e informatici, diretta espressione della diversa tecnologia in gioco. I membri del "club atomico", infatti, sono appena nove[4] e anche gli stati con avanzate capacità nucleari sono un numero circoscritto, senza contare che in linea di massima è tecnicamente agevole individuare da dove sia partito un missile che trasporti una testata nucleare. Tutt'altra storia per quanto riguarda gli attacchi informatici: non solo la struttura della rete e le prevalenti modalità di attacco rendono complesso capire da dove abbia avuto origine un attacco cibernetico, ma i potenziali hacker sono numerosissimi e sparsi in tutto il mondo e non tutti sono espressione di un governo.

A tal proposito è significativo il caso dell'attacco contro l'Estonia del 2007, generalmente considerato il primo attacco cibernetico su larga scala con motivazioni politiche piuttosto che economiche. Il Paese venne infatti colpito da un *distibuted denial of service*, che mise temporaneamente fuori uso siti web e piattaforme online in risposta alla rimozione da parte del governo di Tallinn di una statua di epoca sovietica che commemorava la vittoria contro la Germania nazista. Benché l'Estonia avesse accusato la Russia dell'attacco, questo venne poi attribuito ad attivisti – o meglio "hactivisti" – russi, senza tuttavia poter dimostrare il coinvolgimento del governo di Mosca.

[3] Trey Herr, "PrEP: A Framework for Malware & Cyber Weapons", in *Journal of Information Warfare*, vol. 13, n. 1 (febbraio 2014), p. 87-106.

[4] Stati Uniti, Russia, Regno Unito, Francia, Cina, India, Pakistan, Israele e Corea del Nord.

La capacità di innescare attacchi cibernetici distruttivi da parte di attori privati – e perfino di singoli individui – complica immensamente l'impiego di tutti quegli strumenti che sono stati cruciali per la gestione dei rischi nucleari: da un lato la dottrina della deterrenza, che prevede la minaccia dell'uso di armi nucleari al fine di non doverle mai usare, e dall'altra le norme con le quali sono state regolamentate a livello internazionale, la non-proliferazione e il controllo degli armamenti. Le sezioni seguenti illustreranno in che modo questi tre strumenti, sviluppati per rispondere alle esigenze della realtà nucleare, possano tuttavia avere una rilevanza anche nell'epoca della guerra cibernetica.

4.2 Deterrenza

La deterrenza è una strategia coercitiva che si basa sul principio secondo il quale al fine di ottenere un risultato spesso basta una minaccia, purché credibile. È così che le armi nucleari non sono state mai più lanciate contro un avversario dal 1945, ma hanno continuato a sortire importanti effetti politici. Per uno dei suoi primi teorici, Thomas Schelling[5], la deterrenza è una minaccia che mira a non far compiere a un avversario un'azione indesiderata basandosi sulla "percezione di un avversario che i costi e/o i rischi di un'azione che potrebbe intraprendere sono superiori rispetto agli eventuali benefici"[6]. In ambito nucleare, infatti, i costi inflitti da un contro-attacco nucleare tendono a eccedere i benefici che verrebbero dal lanciare un'offensiva atomica. Ne risulta la famosa immagine evocata dal "padre della bomba", Robert Oppenheimer, di due scorpioni bloccati in un vaso, capaci di uccidersi a vicenda ma solo a rischio della propria stessa vita. In un simile frangente mancano cioè gli incentivi a un comportamento offensivo a causa della propria vulnerabilità a un'azione uguale e contraria. La volontà di sopravvivenza renderebbe dunque irrazionale un attacco nucleare se si può essere soggetti a una controffensiva.

Sono queste le basi della dottrina della "mutua distruzione assicurata" (*Mutually assured destruction*, Mad), che ha caratterizzato la relazione tra Stati Uniti e Unione Sovietica durante la guerra fredda. Secondo molti autori ciò ha reso impensabile l'uso di armi nucleari, prevenendo

[5] Thomas C. Schelling, *La diplomazia della violenza*, Bologna, Il mulino, 1968.

[6] Alexander L. George e Richard Smoke, *Deterrence in American Foreign Policy. Theory and Practice*, New York, Columbia University Press, 1974.

lo scoppio della terza guerra mondiale e garantendo così una situazione di non belligeranza attiva tra le due superpotenze, quella che John Lewis Gaddis chiamò "lunga pace"[7]. Bisogna tuttavia ammettere che l'efficacia della deterrenza – o almeno la fiducia nella sua sicurezza – è stata a più riprese messa in dubbio, sia su un piano teorico che storiografico[8]. A ciò si è aggiunta nel nuovo millennio la preoccupazione che la dottrina Mad non abbia utilità nei confronti di terroristi o altri aggressori di natura non statuale. Quel che è certo è che negli ambienti militari la deterrenza è la chiave interpretativa prevalente per la gestione dei rischi dei rischi nucleari e gioca un ruolo di primo piano nella pianificazione strategica. Ci si è chiesti perciò se anche in caso di minacce cibernetiche possa essere usata la deterrenza e a quali risultati porterebbe.

Si può innanzitutto tracciare una distinzione tra la deterrenza "*by denial*" e "*by punishment*", ovvero per negazione o per punizione: la prima è mirata a fare in modo che un avversario non sia in grado di approfittare di un'opzione strategica, mentre la seconda consiste nel minacciarlo così che non intraprenda un'azione offensiva[9]. La deterrenza per negazione si affida essenzialmente a soluzioni difensive che impediscano di riportare danni ingenti. Sul fronte cyber la negazione delle opzioni strategiche all'avversario si sostanzia attraverso un innalzamento della protezione di reti e sistemi che consenta di gestire il rischio, intercettare eventuali intrusioni e rimanere quanto più possibile immuni. Sembrerebbe andare in questa direzione la recente decisione della Russia di sviluppare un "Internet sovrano", cioè di predisporre la propria architettura delle reti in modo tale da potersi isolare dalla rete globale nel caso di attacchi, facendo confluire tutto il traffico entro i confini nazionali e creando un registro parallelo del web.

---

[7] John Lewis Gaddis, *The Long Peace. Inquiries into the History of the Cold War*, Oxford, Oxford University Press, 1987.

[8] Nina Tannenwald ha dimostrato che non è stata la deterrenza a prevenire diverse situazioni di mancato utilizzo della bomba atomica, quanto piuttosto l'emergere di una prescrizione normativa, un tabù, in tal senso. Dal canto suo, John Mueller ha sostenuto che le armi nucleari siano state irrilevanti nel mantenimento della pace post-1945. Nina Tannenwald, *The Nuclear Taboo. The United States and the Non-Use of Nuclear Weapons since 1945*, Cambridge, Cambridge University Press, 2007; John Mueller, "The Essential Irrelevance of Nuclear Weapons: Stability in the Postwar World", in *International Security*, vol.13, n. 2 (Fall 1988), p. 55-79.

[9] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, RAND Corporation, 2009, p. 27-37, https://www.rand.org/pubs/monographs/MG877.html.

La deterrenza per punizione richiede invece l'istituzione di una minaccia di rappresaglia credibile. Per la cybersecurity ciò vorrebbe dire essere in grado di sopravvivere a un attacco e rispondere colpendo assetti importanti per l'avversario. Per poter contrattaccare, tuttavia, è indispensabile essere in grado di identificare chi sia responsabile dell'aggressione subita, cosa che nel ciberspazio risulta estremamente complessa, come sottolineato in precedenza. Il problema dell'*attribution*, secondo molti, renderebbe la deterrenza inapplicabile a questo dominio. Senza sapere con certezza chi sia il responsabile non si potrebbe effettuare una rappresaglia e si rischierebbe di generare un'escalation nel caso di errori di valutazione. L'incertezza nell'attribuzione degli attacchi finisce quindi per dare all'aggressore un vantaggio, dal momento che può agire nella speranza di non essere individuato e dunque punito. La *plausible deniability* – cioè la possibilità di negare in maniera plausibile di aver commesso un'intrusione cibernetica – minerebbe dunque alla radice i requisiti della deterrenza.

È quindi possibile che si riuscirà a esercitare deterrenza, e a influenzare il calcolo strategico dell'avversario, nella misura in cui lo permetteranno i miglioramenti delle capacità tecniche della *cyber forensics*. Rimangono comunque le difficoltà relative ai diversi corollari alla dottrina della deterrenza – come segnalare quali siano le linee rosse che innescherebbero un attacco, mantenere l'impegno preso e dimostrare credibilità – la cui risoluzione appare problematica.

Occorre infatti ricordare che la deterrenza nucleare, sia in teoria che in pratica, si è ampliata fino a includere la prevenzione di attacchi rivolti non solo contro il Paese che la esercita, ma anche contro i suoi alleati (deterrenza estesa). Nello specifico gli Stati Uniti attraverso la Nato garantiscono protezione agli alleati con tutti i mezzi a disposizione, cosa che pone le basi per una minaccia nucleare in risposta a un attacco contro uno dei suoi membri. Tale dottrina già durante la Guerra Fredda ha sollevato questioni di credibilità visto quanto sarebbe politicamente difficile sopportare una eventuale controffensiva nucleare per difendere un alleato.

L'ombrello nucleare, ad ogni buon conto, forse è già affiancato da un ombrello cyber. La Nato ha stabilito nel 2014 che un attacco cibernetico può portare all'invocazione dell'articolo 5 della Carta Atlantica, la clausola di difesa collettiva. Da allora l'alleanza si sta muovendo per integrare le capacità cyber degli stati membri e, dal 2023, dovrebbe essere operativo il comando cibernetico della Nato. Sarà interessante esaminare, con l'evolversi della dottrina strategica, in che misura l'estensione della deterrenza cibernetica si rivelerà efficace nel prevenire aggressioni contro i membri dell'alleanza.

Si può dunque concludere che l'applicazione della deterrenza all'ambito cyber è estremamente complicata, tanto più in un contesto in cui possa esservi una certa ambiguità rispetto all'interpretazione di un'intrusione cibernetica come attacco armato. Al contrario delle armi nucleari, quelle cyber non hanno ad oggi una capacità di minaccia esistenziale e non raggiungono quindi una soglia di distruttività che conferisce credibilità alla reciproca minaccia e stabilità al sistema. Inoltre, così come in ambito nucleare, la deterrenza è più complessa quando non vi è simmetria tra avversari, caratteristica dominante del ciberspazio[10].

4.3 Non-proliferazione

Alec Ross ha definito lo spazio informatico "un Far West" in cui non vi sono regole e non c'è alcuna autorità preposta a farle rispettare[11]. Ed effettivamente nel ciberspazio la creazione di trattati internazionali o di norme che garantiscano una qualche prevedibilità comportamentale è ancora allo stato embrionale. Lo stesso si poteva dire, tuttavia, del mondo degli anni '50 in cui molti Paesi aspiravano ad acquisire capacità nucleari militari e non esistevano ancora quelle barriere legali che conosciamo oggi e che hanno aiutato a mantenere sotto controllo il numero delle testate atomiche e degli stati che le possiedono.

Al fine di contenere il numero di stati detentori di certe tecnologie particolarmente pericolose e dagli effetti indiscriminati sono stati creati regimi internazionali di non-proliferazione. Ciò è avvenuto non solo per le armi nucleari ma anche per quelle biologiche e chimiche, regolate rispettivamente dalla Convenzione sulle armi biologiche firmata nel 1972 e da quella sulle armi chimiche, sottoscritta nel 1993. Gli effetti di queste armi di distruzione di massa (Adm), infatti, le pongono su un piano diverso rispetto agli strumenti bellici convenzionali e rendono quindi necessaria la loro limitazione. Una limitazione che è riuscita a estendersi alla quasi totalità della collettività internazionale e a contenere lo sviluppo bellico di tali tecnologie[12].

---

[10] Mariarosaria Taddeo, "The Limits of Deterrence Theory in Cyberspace", in *Philosophy & Technology*, vol. 31, n. 3 (settembre 2018), p. 339-355.

[11] Alec Ross, *Il nostro futuro. Come affrontare il mondo dei prossimi vent'anni*, Milano, Feltrinelli, 2016.

[12] La Convenzione sulle armi biologiche è entrata in vigore nel 1975 e ha 182 stati membri. La Convenzione sulle armi chimiche è in vigore dal 1997 e conta 193 stati membri.

In ambito nucleare il concetto di non-proliferazione è stato applicato con l'istituzione di un regime volto a mantenere stabile e contenuto il numero di stati capaci di adoperare tecnologie atomiche per scopi militari. Al centro di tale architettura risiede il Trattato per la non-proliferazione nucleare (Tnp), firmato nel 1968 e giunto ora a coinvolgere 191 stati. Il trattato impone ai suoi membri di non sviluppare armamenti atomici – con l'eccezione dei cinque stati che fino ad allora li avevano già acquisiti[13] – ma viene garantito loro lo sfruttamento pacifico delle tecnologie nucleari. Alla base dell'accordo vi è quindi una basilare discriminazione tra i cosiddetti *haves* e gli *have-nots*, cioè tra chi possiede la bomba e chi non vi può aspirare.

Nonostante il trattato includa una clausola (l'articolo VI) che richiede ai cinque stati nucleari di negoziare l'eliminazione dei loro arsenali, pochi risultati sono stati raggiunti in tal senso. Proprio al fine di superare questa originale discriminazione, stati privi di armi nucleari e attivisti si sono adoperati per creare un nuovo accordo per mettere al bando tutte le armi nucleari, anche quelle dei cinque Paesi cui il trattato "permette" il possesso della bomba e quelle di chi è rimasto fuori dal Tnp (Corea del Nord, India, Israele, Pakistan e Sud Sudan[14]) e non è dunque legalmente vincolato dai suoi termini.

Ogni regime internazionale si regge sulla attrattiva che possiede verso gli stati potenziali sottoscrittori: se pochi firmano un accordo di limitazione delle dotazioni militari gli effetti benefici saranno giocoforza limitati. Il Tnp con la sua ampia *membership* dimostra di avere credibilità presso la comunità degli stati, ma soprattutto la sua vasta estensione ha garantito benefici di sicurezza per tutti i firmatari. Vale la pena ricordare un altro istituto del regime di non-proliferazione, cioè le zone libere da armi nucleari, realizzate grazie ad accordi che, a livello regionale, stabiliscono lo *status* non-nucleare di tutti i Paesi inclusi nella zona. La consapevolezza che un vicino, potenzialmente aggressivo o con cui si condivide un passa-

[13] Stati Uniti, Unione Sovietica, Regno Unito, Francia e Cina.

[14] Il Sud Sudan, che è indipendente dal 2011, è l'unico dei cinque Paesi a non avere armi nucleari ma comprensibilmente la firma del Tnp non è stata tra le sue priorità diplomatiche. Degli altri quattro, la Corea del Nord è stata un membro del Tnp dal 1985 al 2003, quando ha denunciato l'accordo invocandone la clausola di recesso (Articolo X). Tre anni dopo condurrà il suo primo test nucleare. India e Pakistan si sono unite al "club nucleare" nel 1998. Ancora diverso è il caso di Israele che adotta una politica per la quale non conferma né smentisce il proprio possesso di armi nucleari, ma gli esperti concordano che possieda un arsenale di circa 80 bombe atomiche.

to di contese, abbia rinunciato a esercitare una minaccia nucleare è un potente incentivo per fare altrettanto. È questo il caso, ad esempio, di Brasile e Argentina, entrate a far parte del Trattato di Tlatelolco (la zona libera da armi nucleari in America Latina e nei Caraibi) dopo aver rinunciato alle rispettive ambizioni nucleari che, per reciproco timore, avevano coltivato durante il periodo delle dittature militari.

In ambito cibernetico bisognerebbe dunque comprendere come una norma di non-proliferazione si possa tradurre in pratica. A questo proposito è opportuno segnalare che molti ritengono che gli attacchi cyber non raggiungano gli effetti di cui sono capaci le armi di distruzione di massa e non si possa quindi parlare di Adm in questo caso, mentre altri hanno provato a introdurre la categoria di Adm elettroniche[15]. Indipendentemente da questi problemi di definizione, per istituire una proibizione alla proliferazione, sarebbe innanzitutto necessario che gli stati identifichino le tecnologie classificabili come arma cibernetica e impongano che queste non possano essere ulteriormente diffuse. Come già illustrato, non è semplice identificare cosa sia un'arma cibernetica e quindi di cosa esattamente si dovrebbe evitare la proliferazione. Al di là di questo, bisognerebbe definire se la proibizione al possesso si debba applicare a tutti i membri dell'accordo o solo a una cerchia ristretta, cioè se seguire l'esempio delle convenzioni sulle armi chimiche e biologiche oppure quello del Tnp. In questo secondo caso si renderebbe indispensabile non solo trovare un'intesa tra gli *haves* del ciberspazio, ma anche fornire adeguati incentivi per garantire la cooperazione degli *have-nots*.

A completamento delle proibizioni contro la proliferazione di armi nucleari vi sono anche accordi per il controllo delle esportazioni, che proibiscono la vendita a Paesi potenzialmente pericolosi di armi e tecnologia *dual use*, cioè con applicazioni sia civili che militari. I controlli vengono attuati dai singoli stati mediante legislazioni e procedure nazionali, cioè essenzialmente attraverso licenze all'esportazione e ispezioni doganali. Il Nuclear Suppliers Group (Nsg) è stato creato nel 1974 da sette stati esportatori di tecnologie nucleari che volevano evitare il ripetersi del test atomico indiano, test che aveva dimostrato la relativa facilità con la quale dotazioni di natura civile potessero essere velocemente messe a servizio di assetti militari. Con 49 membri, l'Nsg è ora certamente più

[15] Cristian Barbieri, Jean-Pierre Darnis e Carolina Polito, "Non-proliferation Regime for Cyber Weapons: A Tentative Study", in *Documenti IAI*, n. 18|03 (marzo 2018), p. 20, https://www.iai.it/it/node/8870.

efficace nell'impedire l'accesso a tecnologie *dual use* da parte di Stati che potrebbero "militarizzarle". Tuttavia, il regime risente di forti problemi di legittimità, accusato di essere strumento per mantenere un predominio tecnologico sulla maggioranza dei Paesi.

Così come la tecnologia nucleare, anche quella cyber è per sua natura *dual use*, e dunque di difficile limitazione. Si può quindi comprendere come il sistema dei controlli alle esportazioni possa essere il più facilmente "trasferibile" all'ambito cyber tra le componenti del regime di non-proliferazione nucleare. Stilare liste di tecnologie pericolose e richiedere licenze speciali per la vendita oltre confine di software e hardware è tecnicamente possibile e, come per le armi nucleari, i Paesi esportatori di tecnologia cyber sono tuttora un gruppo abbastanza limitato. Difatti dal 2013 il Wassenaar Arrangement[16], uno dei sistemi per i controlli delle esportazioni di Adm, ha introdotto nella lista delle tecnologie di cui è proibito il trasferimento anche alcuni strumenti cibernetici, i software di intrusione (*intrusion software*). Si tratta di tecnologie e software usate per il monitoraggio remoto di computer e telefoni cellulari, cioè spyware e sistemi di sorveglianza avanzati.

Per regolamentare i trasferimenti internazionali di tecnologie cyber potenzialmente utilizzabili in un'arma cibernetica bisognerebbe ampliare ulteriormente tale lista. Ciononostante un simile impianto sarebbe ancor meno giustificabile per tutti quegli stati che aspirano ai benefici delle tecnologie cibernetiche, pur non volendosi necessariamente dotare di una capacità cyber offensiva. La formulazione originaria dell'estensione dell'accordo Wassenaar ai software di intrusione, redatta con scarso riguardo per la dimensione tecnica, aveva finito per rendere inammissibile anche i trasferimenti di tecnologia volti a migliorare le capacità difensive. Da parte privata, infatti, tale mossa è stata contestata in quanto dannosa per i processi di innovazione tecnologica. Al contrario del settore nucleare, in cui la distinzione tra tecnologie di natura offensiva e difensiva può essere tracciata, nel ciberspazio sono spesso identici i sistemi utilizzati per difendersi e per attaccare, cioè per compiere un'intrusione e per prevenirla.

Inoltre, dal momento che sono spesso attori privati a produrre le tecnologie digitali, occorrerebbe garantire la loro cooperazione perché un simile sistema funzioni. Le pressioni del mercato, tuttavia, sembrano incen-

[16] L'intesa di Wassenaar per i controlli alle esportazioni di armi convenzionali e beni e tecnologie dual use è stata sottoscritta nel 1996 e comprende 42 stati membri.

tivare tali aziende ad agire con scarso riguardo delle implicazioni etiche, se non securitarie. Basti pensare ai numerosi casi di aziende che hanno venduto tecnologie di intrusione e spionaggio a governi poco rispettosi dei diritti umani. Nel 2015, ad esempio, una fuga di dati (*data breach*) aveva rivelato come Hacking Team, un'azienda italiana, vendesse soluzioni di sorveglianza a imprese straniere e a diversi governi, inclusi quelli di Sudan, Arabia Saudita, Etiopia e Bahrain. Anche in questo caso lo scarso controllo esercitato dagli stati sulle tecnologie digitali prefigura uno scenario negoziale e attuativo più complesso rispetto a quanto riguarda le tecnologie nucleari.

4.4 Controllo degli armamenti

Diverse rispetto alle norme per contenere il numero di stati in possesso di Adm, sono le regole mirate a limitare il tipo e il numero delle armi permesse a un dato Paese o, più spesso, a un gruppo di Paesi. Il concetto di controllo degli armamenti, secondo la popolare definizione di Schelling e Halperin, si riferisce a misure volte a "evitare una guerra non voluta delle parti, a minimizzare costi e rischi della competizione sugli armamenti e a ridurre la portata e la violenza della guerra se dovesse scoppiare"[17].

Su questi presupposti sono stati creati gli accordi che Stati Uniti e Unione Sovietica (poi Russia) hanno sottoscritto per mettere un freno alla corsa agli armamenti nucleari che aveva portato le due superpotenze ad accumulare oltre 80.000 testate atomiche. A partire dagli accordi Salt (*Strategic Arms Limitation Talks*) degli anni '70 che istituivano tetti massimi per gli arsenali strategici, Washington e Mosca sono riuscite anche a ridurre il numero delle rispettive armi nucleari tramite i trattati Start (Strategic Arms Reduction Treaty). L'ultimo, il New Start firmato nel 2010, impone che non vengano schierati più di 1.550 testate nucleari e più di 700 vettori (missili e bombardieri) per parte.

Tutto ciò ha permesso di bloccare la corsa agli armamenti, introdurre un grado di stabilità e prevedibilità nelle relazioni bilaterali militari, oltre che creare una certa fiducia reciproca. La chiave in tal senso è la "verificabilità" degli accordi, ovvero l'istituzione di meccanismi per il reciproco controllo del rispetto del trattato. Per verificarne l'attuazione il già citato

[17] Thomas Schelling e Morton Halperin, *Strategia e controllo degli armamenti*, Bologna, Il mulino, 1962.

New Start, per esempio, prevede l'utilizzo di satelliti e monitoraggio da remoto, oltre che visite in situ per attestare il rispetto dei limiti. Sistemi intrusivi di verifica sono cruciali anche per la tenuta degli accordi di non-proliferazione esaminati in precedenza, che sono affidati all'Agenzia internazionale per l'energia atomica (Aiea).

La questione delle verifiche rappresenta un'ulteriore criticità nella riflessione sull'applicabilità dei concetti nucleari al mondo cibernetico. In ambito cyber è difficile immaginare che si possano effettuare delle ispezioni intrusive. Non si tratta infatti di contare missili ed esaminarne le caratteristiche, come nelle intese per il controllo degli armamenti, o di pesare materiali fissili o valutarne il grado di purezza, nel caso delle verifiche per gli accordi di non-proliferazione. Si tratta piuttosto di agire su tecnologie virtuali, per loro natura immateriali e replicabili.

Sarebbe inoltre difficile immaginare che uno stato possa accettare di aprire le proprie reti alle ispezioni in maniera completa (l'equivalente delle ispezioni in situ), dal momento che ciò assicurerebbe alla controparte una perfetta conoscenza di vulnerabilità ed eventuali exploit (una porzione di codice che può permettere un'intrusione). Tuttavia, verifiche sarebbero possibili con metodi meno intrusivi, come avviene attraverso satelliti e aerei spia, previsti negli accordi per il controllo degli armamenti nucleari (i cosiddetti mezzi tecnici nazionali). Nel ciberspazio, però, ciò rischia di rendere indistinguibili le attività di monitoraggio del rispetto dell'accordo da quelle volte allo spionaggio[18].

Conclusioni

Dopo aver passato in rassegna i principali strumenti con i quali sono state teorizzate e normate le relazioni nucleari, si possono trarre delle preliminari conclusioni in merito all'analogia tra la gestione del rischio nucleare e di quello cibernetico. Dovrebbe essere chiaro dalla precedente analisi che vi sono differenze intrinseche nelle due tecnologie, che rendono l'applicazione dei concetti nucleari non immediatamente replicabile nel ciberspazio. Nonostante entrambe le innovazioni abbiano prodotto armi capaci di enormi distruzioni, quelle nucleari per loro natura costituiscono una minaccia esistenziale che continua a porle in una categoria diversa

[18] Erica D. Borghard e Shawn W. Lonergan, "Why Are There No Cyber Arms Control Agreements?", in *Net Politics Blog*, 16 gennaio 2018, https://on.cfr.org/2DoQke3.

rispetto a ogni altro strumento bellico. Inoltre, le difficoltà insite nell'attribuzione di episodi di hacking a un determinato gruppo o stato fa sì che le relazioni cibernetiche si caratterizzino per un grado di incertezza e instabilità molto più alto di quello che distingue quelle nucleari.

L'esame della dottrina della deterrenza porta a concludere che la sua applicazione sia ben più complessa in ambito cyber rispetto a quanto avviene in campo nucleare. Occorre segnalare tuttavia che anche la deterrenza nucleare, una sorta di pace armata, è una strategia che, fondandosi sulla possibilità dell'uso della bomba, risulta pericolosa in tempo di pace e può condurre a conseguenze apocalittiche in caso di crisi. Sebbene sia certamente preferibile una situazione in cui l'uso delle armi venga solo minacciato invece che messo in pratica, non per questo è inevitabile che le strategie degli stati si basino sul presupposto dell'uso della forza.

I numerosi accordi nucleari sottoscritti dagli stati, in formato bilaterale o multilaterale, dimostrano che è possibile limitare gli utilizzi di una tecnologia militare. Bisogna ricordare, infatti, che anche all'inizio dell'epoca nucleare sembrava impossibile normare e circoscrivere le ambizioni securitarie degli stati. Ciò non implica che la governance nucleare sia in toto applicabile al ciberspazio e anzi, come la precedente analisi ha illustrato, i problemi relativi alla definizione di cosa costituisce un'arma cibernetica, ai suoi usi sia militari che civili e alle modalità di verifica del rispetto degli impegni sottoscritti ostacolano la creazione di qualunque accordo internazionale per la non-proliferazione o il controllo degli armamenti cyber.

Ogni tecnologia differisce da un'altra e, rendendo possibili diversi tipi di uso della forza, produce effetti sui rapporti tra stati difficilmente comparabili. Questo non dovrebbe però scoraggiare la ricerca di soluzioni innovative per mettere a freno il rischio cibernetico. Le differenze illustrate in queste pagine dovrebbero invece far riflettere su cosa sia necessario per raggiungere accordi che permettano di contenere la specifica pericolosità del ciberspazio. Per esempio, la commistione di interessi pubblici e privati, come a più riprese enfatizzato, rende qualunque tentativo di normare le attività permesse nel ciberspazio una sfida di tutt'altro peso rispetto a quanto avvenuto in ambito nucleare. Ciò mette in crisi il paradigma della responsabilità degli stati e rende necessario espandere la governance dei processi cibernetici a nuove categorie di attori, la cui inclusione è indispensabile ai fini dell'efficacia di ogni limitazione.

Tra gli stakeholder ineludibili ai fini di una regolamentazione del ciberspazio vi sono certamente le aziende private: queste controllano buona parte delle reti e di quel che vi transita, oltre che una vastissima porzione

delle infrastrutture critiche mondiali. Un'altra categoria di attori, spesso ignorata in discussioni di questo tipo, è quella degli scienziati informatici che, come quelli nucleari prima di loro, possono giocare un ruolo di primo piano nella governance cibernetica. In epoca atomica non furono tanto gli stati i primi fautori di un ordine nucleare più controllato. Al contrario, fin dai primi anni della rivoluzione nucleare, furono gli scienziati coinvolti nei progetti bellici a dare un impulso in tal senso.

Alcuni dei fisici nucleari che parteciparono all'invenzione della bomba atomica rimasero talmente colpiti dagli effetti catastrofici di quel che avevano contribuito a generare da attivarsi per il disarmo nucleare. È questo il caso del fisico polacco di passaporto britannico Joseph Rotblat, che abbandonò il Progetto Manhattan quando seppe per certo che la Germania nazista non sarebbe riuscita a far esplodere un proprio ordigno atomico. È anche il caso di Albert Einstein, che animò le prime iniziative per un uso responsabile della scienza nucleare, incluso accettare l'invito di Bertrand Russell a firmare il manifesto con cui i maggiori scienziati dell'epoca chiedevano l'eliminazione della bomba atomica ().

Sulla base del manifesto Russell-Einstein si costituì il movimento delle Pugwash Conferences on Science and World Affairs, una sorta di rete informale per mettere in contatto scienziati provenienti dai due lati della cortina di ferro e che ebbe nello stesso Rotblat una delle figure chiave. Pugwash e altre simili iniziative permisero agli scienziati di sedersi attorno a un tavolo e creare un clima di fiducia tale da consentire l'esplorazione di proposte negoziali su concreti presupposti scientifici. Fu in quella sede, infatti, che emersero gli embrioni di alcuni degli accordi per il controllo degli armamenti discussi in precedenza.

La responsabilità sociale degli scienziati digitali deve dunque essere presa in considerazione per riflettere su come effettuare la transizione dalla situazione attuale a una di maggior moderazione dei rischi cibernetici. Vi sono state alcune iniziative per sensibilizzare agli usi etici della scienza informatica già negli anni '80, come il Forum of Computer Scientists and IT-Professionals for Peace and Social Responsibility in Germania, o il gruppo Computer Professionals for Social Responsibility negli Stati Uniti. Dall'inizio del nuovo millennio è invece attivo il panel permanente per il monitoraggio della sicurezza informatica della World Federation of Scientists che nel 2009 ha lanciato la Dichiarazione di Erice, un appello per evitare la guerra cibernetica. Tuttavia non sembra che queste iniziative abbiano riscosso molto successo né che si possa parlare di un ampio movimento sociale per contenere la dimensione bellica delle tecnologie cyber.

È importante quindi lavorare per il coinvolgimento della comunità scientifica nel dibattito su come istituire un ordine cyber, per quanto limitato, perché solo un sistematico scambio di vedute tra lato tecnico e politico può portare a soluzioni efficaci. Ma è soprattutto importante che, nella corsa allo sfruttamento del ciberspazio, non si dimentichino le dimensioni etiche del lavoro di chi vi è coinvolto. Questo capitolo si chiude quindi con una domanda rivolta a tutti coloro i quali sono impegnati a ideare le nuove applicazioni digitali del futuro: è ancora valido il monito "ricordate la vostra umanità e dimenticate tutto il resto"[19]?

[19] Così recita il manifesto Russell-Einstein: "Nella tragica situazione che affronta l'umanità, noi riteniamo che gli scienziati dovrebbero riunirsi in un congresso per valutare i pericoli che sono sorti come conseguenza dello sviluppo delle armi di distruzione di massa e per discutere una risoluzione […]. Non stiamo parlando, in questa occasione, come membri di questa o quella nazione o continente o fede religiosa, ma come esseri umani, membri della specie umana, la cui sopravvivenza è ora messa a rischio. […] Dobbiamo cominciare a pensare in una nuova maniera. Dobbiamo imparare a chiederci non che mosse intraprendere per offrire la vittoria militare al proprio gruppo preferito, perché non ci saranno poi ulteriori mosse di questo tipo; la domanda che dobbiamo farci è: che passi fare per prevenire uno scontro militare il cui risultato sarà inevitabilmente disastroso per entrambe le parti? […] Facciamo un appello come esseri umani ad altri esseri umani: ricordate la vostra umanità e dimenticatevi del resto." La traduzione del Manifesto è disponibile online: https://www.senzatomica.it/?p=249.

5.
Il futuro dell'Internet governance e le crescenti spinte verso una sovranità cibernetica

Carolina Polito

La gestione della dimensione cibernetica pone attualmente una delle maggiori sfide alle relazioni internazionali e agli equilibri geopolitici globali. Lo spazio cibernetico è diventato, nell'arco di a malapena cinquant'anni dalla sua commercializzazione, l'arena in cui si consuma una tra le più accanite manifestazioni della competizione militare e diplomatica tra stati. Nuove armi cibernetiche, nuovi comandi e nuove dottrine militari stanno proliferando sullo scenario internazionale. Questa competizione tuttavia, lungi dall'essere relegata solamente all'ambito militare, si riversa anche, e forse soprattutto, sugli aspetti di amministrazione e management di questo nuovo spazio: l'Internet governance. Con il temine Internet governance si intende, secondo la definizione fornita nel ambito del World Summit on Information Society (Wsis) del 2005 "lo sviluppo e l'applicazione da parte dei governi, del settore privato e della società civile, nei loro rispettivi ruoli, di principi, norme, regole, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet"[1]. Oggi, il numero di utenti interconnessi nello spazio cibernetico ha superato la soglia dei quattro miliardi e l'interconnessione coinvolge un numero crescente di infrastrutture critiche dalle quali dipende la sicurezza, e finanche la sopravvivenza, della maggior parte degli stati del mondo. Non stupisce quindi che, nell'ultimo decennio, la gestione di Internet abbia accresciuto

[1] Si veda il sito dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione: *Internet Governance*, http://www.isticom.it/index.php/internet-governance.

esponenzialmente la sua rilevanza politica e strategica e sia stata rimessa in discussione da parte dalla comunità internazionale. La governance digitale è passata dall'essere un ambito di scarso interesse per le dinamiche di potere geopolitiche, all'assumere negli anni un ruolo sempre più centrale nel dibatto internazionale. Le fondamenta su cui è costruito il sistema di governance attuale, poste agli albori dello sviluppo di Internet, hanno subito sempre più contraccolpi e Internet da spazio di interazione neutrale è diventato arena per nuove forme di contesa politica[2].

Con il tempo, il dibattito riguardante la governance internazionale di Internet è andato cristallizzandosi intorno a opposte visioni su quale sia il modello più adeguato per amministrare uno spazio cibernetico in così costante espansione e in particolare su quale ruolo debba essere riservato alla sovranità cibernetica e alle prerogative nazionali dei singoli stati[3]. Il capitolo si prefissa in primo luogo l'obiettivo di analizzare il modello di Internet governance vigente e attraverso quale sviluppo storico questo si sia affermato come modello dominante per il management di Internet. Il capitolo tratta quindi lo sviluppo di una narrativa alternativa volta a mettere in discussione questo modello e ad affermare una maggiore prominenza dei singoli stati nazione come attori principali del processo di Internet management. Dopo aver analizzato i più recenti sviluppi in materia di Internet governance, il capitolo esamina infine alcune prospettive per il futuro di questo conteso ambito.

5.1 Le origini del modello multi-stakeholder

L'attuale sistema di governance digitale è nato negli Stati Uniti. Il "giorno zero" di Internet viene generalmente indicato con il 29 ottobre 1969, quando il primo messaggio informatizzato venne inviato da un computer dell'Università della California a Los Angeles ad uno presso lo Stanford Research Institute. Da quel momento lo sviluppo di un network di computer interconnessi venne affidato agli sforzi congiunti della comunità accademica statunitense e del suo apparato militare. Dal 1969 in poi un nu-

[2] Nazli Choucri, *Cyberpolitics in International Relations*, Cambridge, MIT Press, 2012, p. 8.

[3] In questo capitolo si farà riferimento al concetto di sovranità cibernetica solamente nella sua applicazione relativa all'Internet governance. Affrontare il dibattito sulla sovranità cibernetica e la sua applicazione nel diritto internazionale è al di là dello scopo di questa analisi.

mero sempre crescente di computer venne aggiunto all'Arpanet, il primo network sviluppato dall'agenzia governativa Advance Research Projects Agency (Arpa), rinominata Darpa nel 1972 e incaricata dello sviluppo di nuove tecnologie militari per il Dipartimento della Difesa statunitense[4].

Nata quindi come un'iniziativa sotto il controllo del governo federale americano, dall'inizio degli anni '90 Internet venne aperto al settore privato. Tale decisione cambiò radicalmente lo sviluppo della tecnologia ed influenzò profondamente quella che sarebbe diventata la struttura dell'Internet governance. Durante quegli anni di espansione della tecnologia, Internet venne fondato su una governance limitata e ristretta[5]. Il ruolo statale e governativo nella gestione di tale tecnologia venne quindi fortemente ridotto, privilegiando piuttosto l'autonomia e la libertà di azione del settore privato. Internet quindi divenne il luogo dove mettere in pratica le utopie degli anni '90 di un "paradiso libertario di autodeterminazione individuale e riscatto sociale"[6], in cui i governi avessero la minor influenza possibile. Esemplare è stata la "Dichiarazione di indipendenza del ciberspazio" pubblicata nel 1996 da John Perry Barlow il quale, rivolgendosi ai governi del mondo industrializzato, gli "stanchi giganti di carne e acciaio", sosteneva come ogni loro rivendicazione di sovranità non sarebbe stata accettata nello spazio cibernetico e affermava che essi appartenevano ormai a un mondo passato e non erano più i benvenuti nel mondo del futuro che si stava profilando[7]. In parte, tali sentimenti di affrancamento sociale furono il frutto di un tecno-utopismo fondato, come descrive Morozov, su una fiducia nel progresso tecnologico come forza emancipatrice dei popoli derivante dall'ampliamento delle possibilità di comunicazione offerte da Internet[8]. Inoltre, la fase di com-

[4] Barry M. Leiner et al., *Brief History of the Internet*, Internet Society, 1997, p. 3-7, https://www.internetsociety.org/resources/doc/2017/brief-history-internet.

[5] Andrew N. Liaropoulos, *Democracy and an Open-Economy World Order*, Cham, Springer, 2017, p. 25-35.

[6] Fabio Chiusi, "L'utopia di internet oggi è morta. E anche i guru della rete si sono pentiti", in *L'Espresso*, 28 giugno 2017, http://espresso.repubblica.it/visioni/tecnologia/2017/06/28/news/l-utopia-di-internet-oggi-e-morta-e-anche-i-guru-della-rete-si-sono-pentiti-1.304708.

[7] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 8 febbraio 1996. Disponibile nel sito della Electronic Frontier Foundation: https://www.eff.org/it/node/90139.

[8] Evgeny Morozov, *L'ingenuità della rete. Il lato oscuro della libertà di internet*, Torino, Codice, 2011.

mercializzazione di Internet avvenne in un momento storico in cui nella società americana e nella comunità di "pionieri" che fondarono Internet erano prevalenti sentimenti "libertari e anti-autoritari" e una fiducia in un nuovo corso economico volto a promuovere un sempre più limitato intervento statale nell'economia e segnato dall'ondata di deregolamentazioni che aveva colpito l'economia mondiale in generale, e il settore delle telecomunicazioni in particolare[9].

Il risultante modello di governance, su cui si fonda il management della tecnologia digitale ancora oggi, viene comunemente definito *multi-stakeholder*. Il suo principale promotore sono stati gli Stati Uniti insieme a un nutrito gruppo di alleati tra cui Canada, Australia, Giappone e Unione europea. Il modello è fondato sull'idea di compartecipazione alla gestione di Internet di governi, industria privata, società civile, organizzazioni internazionali intergovernative e altri attori non-statali coinvolti e interessati. In pratica, tuttavia, il settore privato e la società civile, data la struttura concettuale del modello *multi-stakeholder* basata sulla natura informale e tecnica delle origini di Internet, hanno svolto il ruolo maggiore nella gestione del mezzo informatico, contribuendo allo sviluppo del software e dei protocolli fondamentali su cui si basa il funzionamento di Internet, nonché della "dorsale informatica", la struttura fisica che lo sorregge[10].

5.2 Funzioni e organi della governance digitale: il ruolo dell'Icann

Molte delle entità e organizzazioni che hanno contribuito allo sviluppo di Internet continuano tutt'oggi a caratterizzarne il management. Tra queste organizzazioni, quella che più di tutte è responsabile dell'operabilità della tecnologia Internet è l'Internet Corporation for Assigned Names and Numbers (Icann), società privata no-profit con sede in California fondata nel 1998 sotto gli auspici del governo statunitense ed in particolare del Dipartimento del Commercio, la cui influenza sulla società verrà appro-

[9] James A. Lewis, "Sovereignty and the Role of Government in Cyberspace", in *The Brown Journal of World Affairs*, vol. 16, n. 2 (Spring/Summer 2010), p. 55-65.

[10] Lorenzo Maria Pupillo, "Verso una nuova governance globale di internet", in *Notiziario Tecnico Telecom Italia*, n. 1/2013, p. 80-92, https://www.telecomitalia.com/content/tiportal/it/notiziariotecnico/autori/p-q-r/lorenzo-maria-pupillo.html.

fondita di seguito. La società ricopre, in particolare, la funzione di amministrazione dei registri di identificatori Internet. Una delle tecnologie fondamentali alla base del funzionamento di Internet si occupa di tradurre i codici alfanumerici prodotti dagli utenti (ad esempio *www.google.it*) anche detti nomi dominio, in codici binari di 0 e 1 che i computer siano in grado di comprendere per reindirizzare l'utente alla pagina desiderata. Icann ha il compito di assicurare che tali nomi dominio siano unici, quindi che l'utente una volta composto il codice alfanumerico possa essere rimandato ad una sola pagina Internet, e che i rispettivi codici binari siano altrettanto unici. Oltre ad amministrare l'assegnazione dei nomi dominio, tra i quali i domini di primo livello (*Top-Level Domain*, Tld) come *.com*, *.org*, ecc., Icann gestisce l'assegnazione dei *root name server*, server responsabili di fornire informazioni riguardanti i Tld, quindi responsabili di reindirizzare le richieste relative a uno specifico Tld al gruppo di nomi dominio di secondo livello corrispondente. Infine, Icann regola l'assegnazione dei blocchi di indirizzi Ip (Internet Protocol)[11], etichette numeriche che identificano invece i dispositivi connessi alla rete informatica. Nel loro insieme, queste funzioni compiute da Icann garantiscono la *universal resolvability*, elemento chiave per la stabilità e il funzionamento su scala globale di Internet in quanto ne assicurano l'interoperabilità e la standardizzazione sulla base di un linguaggio comune. Anche se all'apparenza molto tecniche, le funzioni sottintendono in realtà delle rilevanti implicazioni politiche. A questo proposito, Laura DeNardis descrive una serie di casi che dimostrano il rilievo politico delle funzioni dell'Icann. Tra questi, l'autrice cita il caso di chi tra la United Arlines, la United Emirates Airlines o il Manchester United dovrebbe avere diritto ad ottenere il nome dominio *united.com*. Tutte e tre le organizzazioni sono nella posizione di reclamare la legittimità della loro richiesta, e la decisione su quale di queste eventualmente potrà godere di tale spazio Internet è, in fondo, una scelta politica[12]. Ancora più esemplificativo è il management dei Tld, come dimostra il caso della richiesta di un tribunale statunitense all'Icann di prendere il controllo sul Tld iraniano *.ir* come forma di rivalsa contro il supporto di Teheran a un attentato delle milizie di Hamas a Gerusalem-

[11] Icann, *General ICANN Factsheet*, novembre 2013, https://www.icann.org/en/system/files/files/quick-look-icann-01nov13-en.pdf.

[12] Laura DeNardis, *The Global War for Internet Governance* (video), conferenza al Centre for International Governance Innovation, Waterloo, 9 settembre 2014, https://www.cigionline.org/node/8180.

me[13]. L'allocazione di Tld assume inoltre una forte connotazione politica, sottolinea Madeline Carr, al momento dell'assegnazione di questi a nuovi stati nati dall'esito di guerre civili, come nel caso delle guerre balcaniche, in cui l'Icann si trova sostanzialmente nella posizione di legittimare la creazione di uno spazio cibernetico statale per queste nuove entità[14].

Fino al momento in cui la tecnologia Internet era funzionale soltanto a connettere la ristretta comunità accademica e militare statunitense, un solo individuo, Jon Postel, si occupò di amministrare i registri di identificatori Internet. A seguito della fase di commercializzazione della tecnologia Internet e del conseguente moltiplicarsi delle richieste di indirizzi Ip e nomi dominio, tuttavia, il compito divenne troppo oneroso per un solo soggetto e si manifestò la necessità di trovare soluzioni alternative per coordinare il complesso sistema di Internet governance. Nel 1992 gli Stati Uniti affidarono quindi il compito di gestire il sistema dei nomi dominio e identificatori ad una società privata, la Network Solution. Ben presto però, come osserva Carr, il governo americano si rese conto che la rilevanza politica della materia eccedeva la sua natura tecnica date le "implicazioni per la sovranità e l'economia degli stati e le diversità culturali"[15], e optò per la creazione, nel 1998, dell'Icann. La creazione dell'Icann, continua Carr, soddisfò le ambizioni egemoniche statunitensi in quanto indirizzò il sistema di Internet governance nella maniera che più soddisfaceva i loro specifici interessi nazionali[16]. Robert Keohane e Joseph Nye furono i primi a sottolineare, nel 1998, come il management di Internet non fosse un ambito di azione neutrale, e quanto questo rafforzasse piuttosto le esistenti strutture del potere. Nello specifico, sottolineavano come gli stati che per primi si muovono nel campo della Internet governance, detti *first-movers*, "sono spesso i creatori degli standard e dell'architettura dei sistemi d'informazione"[17] e godono quindi di un vantaggio strategico su-

[13] Laura DeNardis e Francesca Musiani, "Governance by Infrastructure", in Francesca Musiani et al. (a cura di), *The Turn to Infrastructure in Internet Governance*, Basingstoke/New York, Palgrave Macmillan, 2016, p. 3.

[14] Madeline Carr, *US Power and the Internet in International Relations*, Basingstoke/New York, Palgrave Macmillan, 2016, p. 139.

[15] "These governance functions came to be understood as not simply technical, but highly political as well, due to their implications for sovereignty, state economies and cultural distinctions". Ibid., p. 118

[16] Ibid., p. 129.

[17] Robert O. Keohane and Joseph S. Nye, "Power and Interdependence in the Information Age", in *Foreign Affairs*, vol. 77, n. 5 (settembre/ottobre 1998), p. 88.

gli altri. Emblema di tale vantaggio strategico detenuto dagli Stati Uniti è stato il mantenimento, fino al 2016, di una *stewardship* formale della National Telecommunication and Information Administration (Ntia), organo facente capo al Dipartimento del Commercio americano, sulle funzioni dell'Icann, che quindi legava contrattualmente il ruolo dell'Icann nell'operare le funzioni di assegnazione dei nomi dominio alla supervisione del governo Usa.

Da un lato la governance dell'Icann può essere definita come emblematica del modello *multi-stakeholder* e, al riguardo, Milton Mueller e Jisuk Woo sottolineano come Icann sia un organismo auto-regolato, che non ha bisogno di dipendere da nessuna organizzazione intergovernativa per la formulazione di policy[18], affidata invece ad un consiglio direttivo composto da 21 rappresentanti dei diversi stakeholder coinvolti[19]. D'altro lato, tuttavia, la riluttanza del Dipartimento del Commercio a rinunciare al controllo su uno strumento tanto importante per il management globale di Internet, sebbene all'atto della creazione dell'Icann lo stesso Dipartimento avesse previsto di trasferire la sua governance verso un organismo completamente indipendente "il più presto possibile"[20], ne ha progressivamente minato la legittimità agli occhi di parte della comunità internazionale. Oltre che per la percepita egemonia americana su un organismo con responsabilità dal crescente valore politico, la legittimità dell'Icann è stata inoltre messa in discussione per il processo decisionale interno allo stesso, in quanto sia la trasparenza di tale processo, effettuato a porte chiuse e da membri del consiglio direttivo nominati e non eletti, che l'*accountability* dell'istituzione sono state più volte messe in discussione[21].

5.3 L'Itu e le opposizioni alla governance dell'Icann

Con l'espandersi dello spazio digitale alla fruizione da parte di un numero sempre maggiore di stati il modo in cui tale spazio è governato (e quindi

[18] Milton L. Mueller e Jisuk Woo, "Spectators or Players? Participation in ICANN by the 'Rest of the World'", in William J. Drake e Ernest J. Wilson (a cura di), *Governing Global Electronic Networks. International Perspectives on Policy and Power*, Cambridge/London, MIT Press, 2008, p. 507-533.

[19] ICANN, *General ICANN Factsheet*, cit.

[20] Madeline Carr, *US Power and the Internet in International Relations*, cit., p. 135.

[21] Ibid., p. 137-138.

il modo in cui il pool di risorse digitali disponibili vengono distribuite) ha suscitato crescenti critiche da parte degli stati che si sono sentiti esclusi o danneggiati dal sistema di governance, con Russia e Cina in prima linea nell'opporsi a tale sistema. Due sono le principali obiezioni sollevate dagli stati che hanno più contrastato il sistema di Internet governance.

In primo luogo è stato affermato che il sistema non aveva garantito un livello di sicurezza sostenibile per gli stati che sempre di più dipendono dalla tecnologia Internet e che aveva al contrario contribuito alla proliferazione della minaccia cibernetica alla quale assistiamo oggi. Nato infatti per collegare la comunità ristretta e omogenea dei "pionieri", lo spazio cibernetico non fu sviluppato con in mente la prerogativa della sicurezza, quanto piuttosto quella della sua funzionalità e della possibilità di muovere informazioni in modo veloce e affidabile[22]. Come affermato dallo stesso Vinton Cerf, che insieme a Bob Khan si occupò di progettare negli anni '70 i principali elementi costitutivi del moderno Internet: "All'inizio non ci siamo concentrati su come si potesse distruggere il sistema. Col senno di poi direste che avremmo dovuto farlo, ma all'epoca era difficile perfino farlo funzionare"[23]. Come altre tecnologie in passato, sostiene James Lewis, i vantaggi e i benefici che si prefiguravano con l'avvento di Internet erano tali da affrettarne l'adozione a scapito di considerazioni relative alla sua sicurezza. Per alcune tecnologie, quali quelle aereospaziali, la sicurezza venne successivamente garantita attraverso la combinazione di azioni governative e accordi interstatali, ma per le altre le specificità dell'Internet management, e in particolar modo i limiti posti alla sovranità statale nello spazio cibernetico, hanno impedito un simile sviluppo in termini di garanzie di sicurezza[24]. Tali problematicità sommate alla diffusione non regolata e non pianificata di Internet sono quindi in parte alla base dell'estrema vulnerabilità dello spazio cibernetico. Molti stati hanno sostenuto che in assenza di un adeguato intervento statale il problema della sicurezza restava inevitabilmente irrisolto.

In secondo luogo è stata sollevata una questione di legittimità del modello di governance digitale. Un crescente numero di stati ha manifestato insoddisfazione per non aver partecipato alla creazione del sistema di governance sostenendo che ciò impediva l'adeguata rappresentazione dei

[22] James A. Lewis, "Sovereignty and the Role of Government in Cyberspace", cit.

[23] Craig Timberg, "A Flaw in the Design", in *The Washington Post*, 30 maggio 2015, https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1.

[24] James A. Lewis, "Sovereignty and the Role of Government in Cyberspace", cit.

loro interessi specifici. La governance digitale è stata quindi percepita come un'emanazione della volontà e delle prerogative particolari del governo statunitense.

La prima occasione in cui queste critiche vennero espresse in modo organizzato e sistematico da un gruppo di stati è stata nel contesto del Wsis. Il vertice organizzato dall'International Telecommunication Union (Itu), l'agenzia delle Nazioni Unite responsabile per la definizione di standard internazionali per le telecomunicazioni, si svolse nell'arco di due incontri tenutisi rispettivamente a Ginevra nel 2003 e a Tunisi nel 2005 ed aveva come scopo primario quello di affrontare il tema del *digital divide* e di decidere come sostenere lo sviluppo di tecnologie Ict nei Paesi in via di sviluppo. Durante la fase tunisina del vertice, tuttavia, il focus della conferenza si spostò repentinamente verso il tema dell'Internet governance. Un gruppo di Paesi guidati dal Brasile decise di denunciare l'eccessivo potere degli Stati Uniti rispetto agli altri stati, soprattutto in riferimento al loro ruolo all'interno dell'Icann. Il delegato brasiliano sottolineò come il *digital divide* non fosse un concetto legato esclusivamente all'accesso alle tecnologie informatiche, quanto piuttosto alle "disuguaglianze politiche che si manifestano nell'impossibilità dei Paesi in via di sviluppo di influenzare il processo di *decision-making*"[25].

Il momento più emblematico e più citato in tema di contrasto al sistema di Internet governance è però senza dubbio la World Conference on International Telecommunications (Wcit), conclusasi a Dubai il 14 dicembre 2012. Le negoziazioni in occasione della conferenza tra i 151 Paesi delle Nazioni Unite sono infatti generalmente assurte come la dimostrazione più emblematica delle divergenti visioni sull'Internet governance.

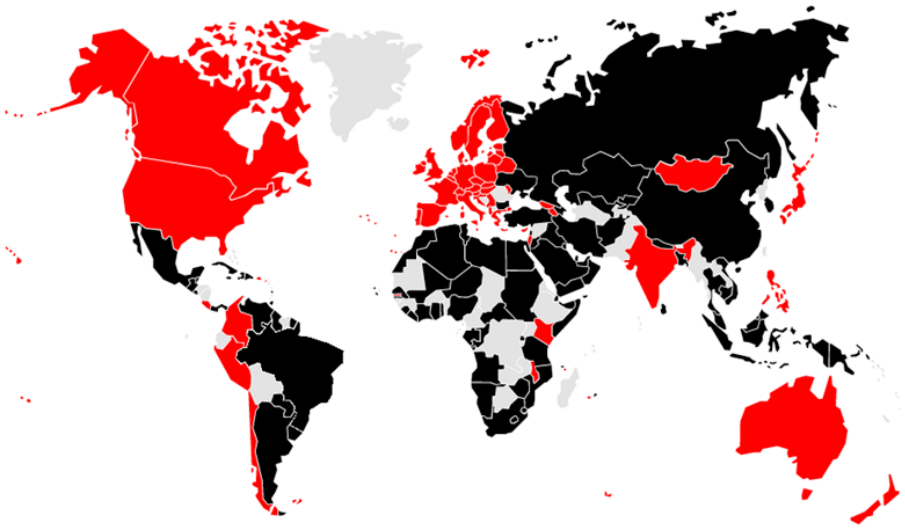
La conferenza organizzata dall'Itu aveva come principale obiettivo quello di ridefinire il regolamento delle telecomunicazioni internazionali (Itr), stipulato nel 1988, alla luce dei più recenti sviluppi relativi a estensione e pervasività di Internet. Una coalizione di stati favorevoli alla definizione di un più chiaro e prominente ruolo dello stato nazione nell'Internet governance era guidata da Russia e Cina. Un secondo gruppo favorevole invece a un sostanziale mantenimento dello status quo, alla difesa delle prerogative del settore privato in materia e a una maggiore liberalizzazione del mercato delle telecomunicazioni[26] annoverava, tra gli

[25] Carol M. Glen, "Internet Governance: Territorializing Cyberspace?", in *Politics & Policy*, vol. 42, n. 5 (ottobre 2014), p. 648.

[26] Ibid., p. 645.

altri, Stati Uniti, Regno Unito, Canada e Australia. Le negoziazioni si conclusero con un risultato clamoroso per la storia dell'Itu: per la prima volta gli stati non riuscirono a raggiungere un consenso e agli 89 firmatari del trattato si contrappose l'oltranzismo del blocco liberale e democratico di 55 membri che decisero di rigettare il trattato e non firmare il documento finale[27].

Figura 6 – Posizione su Itr durante il Wcit 2012



Nota: Rosso = non firmatari; nero = firmatari; grigio = Paesi non Itu.
Fonte: Sangbae Kim, "Cyber Security and Middle Power Diplomacy: A Network Perspective", in *The Korean Journal of International Studies*, Vol. 12, No. 2 (dicembre 2014), p. 340, https://doi.org/10.14731/kjis.2014.12.12.2.323.

Nello specifico la posizione del blocco democratico (occorre sottolineare come alcuni stati a tradizione democratica quali ad esempio Brasile e Corea del Sud abbiano votato a favore del testo finale) affermava che la revisione delle regole Itr così come proposta rappresentava un pericoloso tentativo di minare la libertà di espressione online a vantaggio di potenze autoritarie e della loro capacità di censurare i contenuti online. Due risoluzioni vennero più di tutte contestate dai Paesi non firmatari: la risoluzione 3, dal titolo "*To Foster an Enabling Environment for the Greater Growth of the Internet*", venne criticata in quanto invitava gli stati membri a svolgere

[27] Richard Hill, "WCIT: Failure or Success, Impasse or Way Forward?", in *International Journal of Law and Information Technology*, vol. 21, n. 3 (autunno 2013), p. 314-315.

un ruolo più attivo nel dibattito in materia di Internet governance e a utilizzare nello specifico l'Itu come canale prioritario[28]. Va sottolineato come il blocco facente capo a Russia e Cina avesse individuato proprio nell'Itu la possibile alternativa all'egemonia dell'Icann nel management di Internet. L'Itu, in quanto organismo delle Nazioni Unite, rappresentava infatti per loro l'alternativa multilaterale al modello *multi-stakeholder*. In particolare, il modello decisionale delle conferenze plenipotenziarie, durante le quali solo gli stati membri possono partecipare e votare sulla base del principio "un paese, un voto", e in cui vengono definite le future direzioni di policy dell'Itu, determina la natura multilaterale dell'istituzione in contrapposizione a quella più indiretta ed informale dell'Icann. In aggiunta, i Paesi non firmatari evidenziarono la propria insoddisfazione anche riguardo alle previsioni della risoluzione 5 che, come sottolineato da Pupillo, delegava particolari poteri al Gruppo di studio 3 dell'Itu-T nel predisporre adeguate linee guida per gli stati membri per la regolamentazione dei rapporti commerciali tra le agenzie operative autorizzate e i provider di servizi di telecomunicazioni[29]. Le difficili negoziazioni intorno alle risoluzioni sfiancarono qualunque tentativo di raggiungere un consenso, e delinearono le posizioni di voto sulle quali poi si arroccarono gli stati membri.

5.4 L'Internet governance post-Snowden

La storia recente dell'Internet governance intraprende una repentina inversione di rotta quando, nel 2013, Edward Snowden fa luce sull'estensiva campagna di sorveglianza che il governo degli Stati Uniti, e in particolare la National Security Agency (Nsa), portava avanti in numerosi Paesi. Alla luce di queste rivelazioni il governo e le compagnie Internet americane, accusate di aver collaborato con l'Nsa nel portare avanti la massiva campagna di sorveglianza[30], si trovarono in una posizione particolarmente scomoda per lo strapotere americano nel management di Internet. Vista la crescente perdita di credibilità, sia agli occhi degli utenti di Internet che di altri stati, il governo americano decise di dare avvio al processo di globalizzazione dell'Icann, e alla cessione della sua *stewardship* sulle sue

[28] Lorenzo Maria Pupillo, "Verso una nuova governance globale di internet", cit., p. 83.

[29] Ibid.

[30] Arvind Gupta e Cherian Samuel, "A Comprehensive Approach to Internet Governance and Cybersecurity", in *Strategic Analysis*, vol. 38, n. 4 (2014), p. 591.

attività. Secondo Shwan Powers e Michael Jablonski gli Stati Uniti hanno "dissipato il proprio capitale diplomatico, militare o economico necessario per imporre l'ottemperanza internazionale con il loro controllo unilaterale sul più critico mezzo di comunicazione globale"[31]. Il primo passo verso l'internazionalizzazione dell'Internet management è stato fatto in occasione di un incontro tenutosi il 7 ottobre 2013 a Montevideo, durante il quale i leader dell'Icann, insieme ad altri rappresentanti delle maggiori organizzazioni in capo all'Internet governance, si pronunciarono a favore di tale processo di globalizzazione e di una governance digitale alla quale tutti gli stakeholder potessero partecipare su un piano paritario[32]. Nei tre anni che seguirono tale processo venne avviato e completato, portando a una Internet governance profondamente riformata e tuttavia non meno soggetta alle spinte di sovranità degli stati coinvolti.

Questo processo di globalizzazione dell'Internet governance ha avuto due importanti conseguenze sulle dinamiche geopolitiche che sottintendono la materia. La prima è stata la cessazione della *stewardship* americana sull'Icann, che ha senza dubbio risparmiato a quest'ultimo di stare sotto ai riflettori della politica ai quali negli anni era stato esposto e ha limitato in modo sostanziale il dibattito concernente la sua legittimità nel management di Internet. La seconda è stata la scelta del governo americano di ripiegare dal suo ruolo egemone nel campo della Internet governance, che ha aperto un vacuum politico ben presto riempito da crescenti tendenze alla regionalizzazione dell'Internet governance e all'affermarsi degli interessi particolari degli stati in materia. Tendenza distinguibile non solo tra gli stati storicamente più critici rispetto all'assetto dell'Internet governance, come Russia, Cina, India o Brasile ma anche nell'Unione europea, che ha visto in questi sviluppi un'occasione per riaffermare la propria indipendenza e autonomia decisionale. Inoltre, molti Paesi in via di sviluppo in procinto di informatizzare compiutamente le loro società sono sempre più perplessi sull'idea di adottare un sistema di Internet governance cui essi non hanno contribuito direttamente[33]. Infine, gli Stati

[31] Shawn M. Powers e Michael Jablonski, *The Real Cyber War. The Political Economy of Internet Freedom*, Champaign, University of Illinois Publications, 2015, p. 130.

[32] Icann, *Montevideo Statement on the Future of Internet Cooperation*, 7 ottobre 2013, https://www.icann.org/news/announcement-2013-10-07-en.

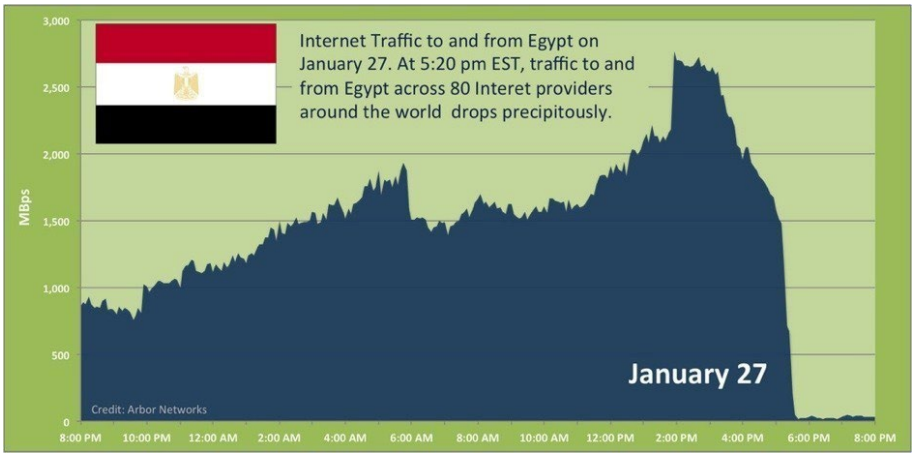
[33] Samantha Bradshaw et al., "The Emergence of Contention in Global Internet Governance", in *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance*, Waterloo/London, Centre for International Governance Innovation/Chatham House, 2016, p. 57, https://www.cigionline.org/node/12252.

Uniti hanno intrapreso una china discendente, verso una sempre maggiore riaffermazione del loro unilateralismo nazionale.

5.5 Sovranità e spazio cibernetico

La prima area in cui si riafferma la sovranità degli stati nello spazio cibernetico è sicuramente quella relativa alle tematiche di sicurezza. In questa narrativa si inseriscono tutte le iniziative più squisitamente militari e che fanno quindi riferimento alla proliferazione nello scenario internazionale di cyber comandi nonché le iniziative volte a diminuire la dipendenza statale da tecnologie e standard stranieri. Mueller sottolinea come le scelte del settore pubblico e privato e le acquisizioni aziendali in materia vengano sempre più di frequente passate al vaglio dai legislatori[34]. Emblematica in tal senso è la decisione del maggio 2019 da parte degli Stati Uniti di inserire la compagnia cinese di telecomunicazioni Huawei nella lista di aziende con cui le compagnie americane possono fare affari soltanto previo consenso[35]. Nella stessa ottica può essere inoltre letto il Mlps (*Multi-Level Protection Scheme*) cinese, con il quale si richiede che i prodotti

Figura 7 – Traffico Internet da e per l'Egitto, 27-28 gennaio 2011



Fonte: Shawn M. Powers e Michael Jablonski, *The Real Cyber War*, cit., p. 167.

[34] Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Cambridge, Polity, 2017.

[35] "Huawei Has Been Cut Off from American Technology", in The Economist, 25 maggio 2019.

It usati dal governo e dalle compagnie nazionali responsabili per le infrastrutture critiche del Paese, come banche e compagnie di trasporti, siano forniti esclusivamente da compagnie It cinesi[36]. Si assiste inoltre a un proliferare di norme attraverso le quali i governi si riservano la possibilità, sempre in nome della sicurezza nazionale, di eseguire arresti temporanei di Internet. In Egitto, durante le rivolte popolari contro il presidente Hosni Mubarak del 2011, l'utilizzo di Internet venne fortemente limitato e messo sotto controllo dalle autorità egiziane per cinque giorni, durante i quali l'accesso alla maggior parte dei siti istituzionali, così come a buona parte dei domini *.eg* venne bloccato[37].

Un'altra area in cui si esprime la sempre maggiore tendenza degli stati di asserire la propria sovranità è quella della territorializzazione del flusso di informazioni. Una serie di iniziative hanno, in questo senso, iniziato a proliferare sullo scenario internazionale, da proposte volte a rafforzare il controllo statale sui contenuti che circolano online, a nuove leggi sulla *data-localization*. In merito alle prime, se il caso più rappresentativo è quello del *Great Firewall* cinese, occorre sottolineare come sempre più Paesi si riservino di prevenire l'accesso dei loro cittadini a contenuti ritenuti illegali, o sgraditi per l'interesse dello stato. Nella sola prima metà del 2017 Google, Facebook e Twitter hanno ricevuto un totale di 114.169 richieste per rimuovere contenuti online da parte di 78 stati e 179.180 richieste per ricevere informazioni riguardanti utenti da parte di 110 Paesi[38]. In merito poi alle crescenti spinte verso la localizzazione dei dati degli utenti entro i confini nazionali, si segnala, ad esempio, l'iniziativa dell'aprile 2018 della Reserve Bank of India che ha richiesto alle società di pagamenti estere di conservare tutti i dati relativi alle transazioni che coinvolgono cittadini indiani esclusivamente in server presenti sul territorio nazionale[39]. È evidente come tali spinte verso politiche di *data-localization* siano il prodotto della reazione internazionale alle rivelazioni di Snowden, e riflettano le preoccupazioni in merito alla capacità degli Stati Uniti di raccogliere intelligence su cittadini stranieri. In questo stes-

[36] Milton Mueller, *Will the Internet Fragment?*, cit.

[37] "L'Egitto spegne Internet", in *Il Post*, 28 gennaio 2011, https://www.ilpost.it/?p=355419.

[38] Roxana Radu, *Negotiating Internet Governance*, Oxford, Oxford University Press, 2019, p. 167.

[39] Ronak D. Desai, "India's Data Localization Remains a Key Challenge for Foreign Companies", in Forbes, 30 aprile 2019, https://www.forbes.com/sites/ronakdesai/2019/04/30/indias-data-localization-remains-a-key-challenge-for-foreign-companies.

so contesto, l'Europa ha anch'essa lanciato il Gdpr con il fine di governare i temi relativi alla privacy, protezione e trasferimento dei dati di cittadini europei. Tra gli aspetti più ragguardevoli dell'iniziativa europea troviamo il focus sul consenso degli utenti al trattamento dei propri dati, e la formulazione del diritto alla rettifica e cancellazione dei dati. Sebbene sia importante evidenziare come l'approccio europeo sia maggiormente indirizzato a garantire la sicurezza dei dati, piuttosto che a stabilire una sovranità su questi, il Gdpr appare comunque come un esempio degno di nota circa la crescente regionalizzazione dei temi di Internet governance di cui prima.

L'ultima area a cui è necessario fare riferimento riguardo l'affermazione della sovranità nazionale nello spazio cibernetico attiene ai tentativi di uniformare le risorse critiche di Internet con i confini nazionali. Con risorse critiche di Internet si intendono tutte quelle funzioni descritte in precedenza in questo capitolo il cui management è di competenza dell'Icann. In quest'area di azione possono essere quindi classificate tutte quelle iniziative volte a detenere un maggior controllo statale sull'assegnazione dei nomi dominio o sul management degli indirizzi Ip. Rappresentativo è il caso della proposta cinese, che non ebbe tuttavia successiva attuazione, intitolata *DNS Extension for Autonomous Internet* presentata alla Internet Engineering Task Force del 2012. La proposta suggeriva di garantire ad ogni nazione la possibilità di stabilire una gerarchia nazionale di nomi dominio e *root server*, permettendo quindi a ciascun Paese di creare i propri Tld, senza la necessità di dover coordinare tale creazione con l'Icann o altre entità sovranazionali[40]. Un caso analogo è quello della nuova legislazione russa in materia di Internet la quale sebbene abbia come scopo principale quello di incrementare la resilienza interna del sistema, fa anch'essa riferimento allo sviluppo di un nuovo sistema di nomi dominio e *root server*[41].

I recenti sviluppi in materia di Internet governance descritti lascerebbero quindi prospettare un futuro di crescente frammentazione di Internet. Nell'immaginare l'Internet del 2029, Michael Grothaus tratteggia un nuovo mondo in cui la rete globale è stata suddivisa in una serie di intranet nazionali, in cui i messaggi via-Internet raggiungono il destinatario

[40] Milton Mueller, *Will the Internet Fragment?*, cit., p. 37

[41] Wolfgang Kleinwächter, "Internet Governance Outlook 2019: Innovative Multilateralism vs. Neo-Nationalistic Unilateralism", in *CircleID*, 8 gennaio 2019, http://www.circleid.com/posts/20190108_internet_governance_2019_innovative_multilateralism_vs_neo.

solo se questo si trova in un Paese alleato con cui sono stati firmati specifici accordi, e in cui l'America ha costruito un muro digitale per evitare gli attacchi informatici internazionali dopo un attacco sferrato contro i suoi sistemi di *smart car* che ha causato decine di migliaia di vittime[42]. Ancorché sia plausibile, come fa Grothaus, immaginare un futuro in cui le possibilità di comunicazione tra i Paesi vengano ridotte a seguito di politiche nazionaliste e isolazionistiche, occorre tuttavia precisare come le possibilità che gli stati prefigurino maggiori vantaggi nel frammentare in modo irreversibile Internet rispetto ai costi che tale scelta comporterebbe, rimangono limitate[43]. I benefici portati dall'interconnessione globale in termini economico-finanziari, e l'accresciuta interdipendenza che ne consegue, non sembrano infatti suggerire la percorribilità di questa strada. Al riguardo la legge di Metcalfe sottolinea come i benefici che gli utenti traggono dallo stare nello stesso network sono proporzionali al numero di persone che condividono tale network. Questa situazione di interdipendenza tra i consumatori di Internet, definita come economia di rete, contribuisce in modo sostanziale a rendere vani gli sforzi nazionali verso una sistematica rottura della compatibilità tecnica dello spazio cibernetico, come quelli verso una nazionalizzazione del sistema dei nomi dominio[44]. Questo è tanto più valido soprattutto perché gli stati godono già della possibilità di censurare o filtrare i contenuti circolanti nello spazio cibernetico nazionale senza dover ricorrere ad una frammentazione tecnica dello stesso, il che riduce l'appeal politico di tale strategia anche per quegli stati di stampo autoritario che hanno maggiore interesse a controllare il flusso di informazioni circolante nei confini nazionali.

Conclusioni

Posta l'improbabilità di una frammentazione tecnica di Internet, è indubbio che i descritti sviluppi in termini di crescenti tendenze da parte degli stati verso una nazionalizzazione dello spazio cibernetico vadano seriamente presi in considerazione e impongano un ripensamento dell'Internet governance rispetto a come questa è stata concepita finora. Particolarmente rile-

[42] Michael Grothaus, "Get Ready for the 'Splinternet': The Web Might Not Be Worldwide Much Longer", FastCompany, 9 luglio 2018, https://www.fastcompany.com/90229453.

[43] Milton Mueller, *Will the Internet Fragment?*, cit.

[44] Ibid.

vante è da considerarsi la dichiarazione del presidente francese Emmanuel Macron in occasione dell'Internet Governance Forum tenutosi a Parigi lo scorso anno con la quale sosteneva la necessità di creare un nuovo modello di multilateralismo. Nello specifico, Macron afferma l'urgenza di superare la "falsa" dicotomia con cui viene concepita la governance di Internet, dove solo due modelli sembrano poter esistere: "da una parte una completa autogestione, senza governance, e dall'altra un Internet frammentato e pienamente controllato da stati forti ed autoritari". Il discorso fa inoltre esplicito riferimento alla carenza di rappresentatività democratica del modello di governance californiano, spesso dominato da colossi privati i quali, sebbene abbiano dato un contributo indispensabile allo sviluppo e funzionamento di Internet, non sono tuttavia stati eletti democraticamente[45].

Alla luce di queste considerazioni, una nuova governance digitale dovrebbe quindi evitare di demonizzare l'intervento statale ma massimizzarne l'utilità. Un tale esercizio volto a ripensare l'Internet governance dovrebbe essere quindi indirizzato verso due paralleli sviluppi. Da un lato, maggiori sforzi dovrebbero essere intrapresi per garantire una migliore *accountability* e rappresentatività degli organi esistenti, primo fra tutti l'Icann. D'altro lato, si potrebbe immaginare un modello di governance "differenziata", attraverso la quale trovare quali siano i confini appropriati per l'intervento statale nell'operare circa i problemi più cogenti per gli interessi nazionali, quali ad esempio temi relativi alla protezione dei dati dei cittadini e alla riduzione della circolazione di discorsi d'odio e disinformazione, immaginando in questo contesto nuove forme di governance condivisa. Altri temi, più tecnici in natura, potrebbero invece continuare ad essere di competenza esclusiva di organi quali l'Icann. Una strategia differenziata permetterebbe di garantire una maggiore democraticità del processo decisionale, riducendo così l'appeal della retorica stato-centrica agli occhi di tutti quegli stati che hanno dimostrato un'attitudine storicamente ambivalente circa questi temi, come ad esempio Brasile e India. Per quanto concerne l'Unione europea, inoltre, questa strategia permetterebbe di garantire maggiori margini di autonomia decisionale e di salvaguardia dei propri interessi specifici, riducendone la dipendenza dai dettami delle due superpotenze.

[45] Speech by M. Emmanuel Macron, President of the Republic at the Internet Governance Forum, 12 novembre 2018, https://www.elysee.fr/en/emmanuel-macron/2018/11/12/speech-by-m-emmanuel-macron-president-of-the-republic-at-the-internet-governance-forum.

6.
Le smart city e la sicurezza: sfide e opportunità per le metropoli mondiali del futuro

Cristian Barbieri

La tecnologia al servizio dell'individuo è un *leitmotiv* che si riproduce in ogni complessità della vita umana. Le città di tutto mondo non sono esenti dagli sforzi dell'uomo di adattare la tecnologia alle richieste dei cittadini. Le dimensioni delle metropoli continuano ad aumentare e secondo le stime delle Nazioni Unite il 55 per cento della popolazione mondiale vive già in una città, con percentuali destinate a salire ad oltre il 68 per cento entro il 2050[1]. La struttura di una città si ritrova quindi pressata da esigenze e attività nuove che devono essere gestite e garantite dagli amministratori locali. Il tutto è anche divenuto un campo prolifico per nuovi business e spazio di ricerca per le aziende multinazionali sempre attenti a opportunità di profitto. A ciò si aggiungano anche i rischi globali legati all'inquinamento e allo spreco di risorse, elementi dall'impatto chiave per una città metropolitana. Gestire un'enorme quantità di persone, e conseguentemente di dati ad essi associati, quindi, diviene sempre più un compito fondamentale per l'amministratore pubblico. Su questo connubio di necessità si incontrano le possibilità di rendere una città *smart*. Ma cosa si intende per città smart?

[1] Undesa, *68% of the World Population Projected to Live in Urban Areas by 2050, Says UN*, 16 maggio 2018, https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html.

6.1 Verso una definizione omnicomprensiva di smart city

Per comprendere interamente le potenzialità e per circoscriverne le applicazioni, occorre quindi definire il termine smart city.

Il vocabolo inizia a circolare tra commentatori internazionali nell'ultimo decennio del secolo scorso, ma è solo con i primi anni duemila che si inizia a concepire cosa e come dovrebbe essere una città smart.

Per iniziare, è bene fare un distinguo dalla città digitale: intesa come la digitalizzazione di alcuni servizi della città, essa può essere una delle componenti della smart city ma non ne è un sinonimo. Importante anche sottolineare che la smart city non è una *intelligent city*. Se in italiano nella traduzione con il lemma intelligente i due termini anglosassoni possono considerarsi sinonimi, in inglese l'accezione *smart* differisce molto da *intelligent* volendo significare che la città non solo possiede tecnologia ma è anche capace di integrarla nei suoi sistemi e di sfruttarla a dovere. L'accezione da intendere è quindi quella di una città intelligente sì, ma anche pratica, capace e reattiva nell'utilizzo di tale tecnologia[2]. Bisogna quindi immaginare un sistema di sistemi all'interno della città capace non solo di immagazzinare dati ma anche di trattarli e renderli disponibili alla collettività per aumentarne il benessere.

Un sistema quindi auto-monitorante e auto-rispondente come ipotizzato da Robert Hall, che però nella sua definizione si focalizza puramente sul monitoraggio e l'integrazione delle condizioni di tutte le infrastrutture critiche[3]. Se le infrastrutture critiche sono un pezzo fondamentale del puzzle di cui è composta una smart city, anche altri tipi di infrastrutture e soprattutto di servizi sono da inserire all'interno di una definizione omnicomprensiva, basti pensare al monitoraggio del traffico nelle arterie principali della città.

Una delle accezioni con cui si può leggere il concetto di smart city è anche quello di pianificazione urbana, difatti si è pensato soprattutto nel primo decennio degli anni 2000 ad etichettare un certo tipo di progetti come smart city. Non solo per la creazione di nuovi quartieri, ma anche

[2] Edoardo Ferrero, "Le smart cities nell'ordinamento giuridico", in *Foro Amministrativo*, a. 2, fasc. 4 (2015), p. 1267-1286, http://hdl.handle.net/2318/1569470.

[3] Robert E. Hall et al., *The Vision of a Smart City*, contributo al 2° International Life Extension Technology Workshop, Parigi, 28 settembre 2000, https://www.osti.gov/servlets/purl/773961.

per utopici progetti di creazione di città smart da zero, in quella prosecuzione culturale discendente dal *genius loci* romano, mai effettivamente compiuti. È il caso della PlanIT Valley, città progettata da giganti hi-tech come Cisco e Ibm nel comune di Paredes in Portogallo e mai realizzata[4]. In questa accezione, il concetto di smart city appare quindi come una semplice etichettatura urbana, intesa come proposta tendente al marketing che vede una città possedere la qualità "smart" così da essere vivibile. In questo testo cercheremo di evitare tale visione e di concretizzare il più possibile l'argomento.

Nel contesto italiano, il vocabolo viene inserito nella categoria neologismi della Enciclopedia Treccani nel 2012 con la seguente dicitura "Città caratterizzata dall'integrazione tra saperi, strutture e mezzi tecnologicamente avanzati, propri della società della comunicazione e dell'informazione, finalizzati a una crescita sostenibile e al miglioramento della qualità della vita"[5].

Nella definizione della Treccani si possono già individuare due componenti e un processo sostanziali della smart city: il fattore umano, il "sapere" nella definizione della Treccani, deve essere in grado di gestire e utilizzare strutture e mezzi tecnologicamente avanzati, cioè l'infrastruttura. In questa definizione manca però l'aspetto istituzionale, quindi l'amministrazione locale, vero abilitatore e gestore, successivamente, della politica smart riguardante la città. Se è vero che da un lato senza individui capaci, siano essi personale tecnico della città o professionisti di aziende fornitrici di servizi, e senza i servizi stessi, una città smart non può esistere, è pur vero che senza l'impulso, in termini economici e pratici, di una pubblica amministrazione efficiente e visionaria nella progettazione e nello stanziamento di fondi in ricerca e sviluppo tecnologico le due componenti da sole non possono ritenersi sufficienti.

La smart city è quindi un luogo fisico, una città, dove le necessità dei cittadini e delle istituzioni sono risolte attraverso un uso smart della tecnologia, un posto quindi in cui network e servizi sono più efficienti che altrove e grazie ai quali il benessere del cittadino ne trova giovamento. È proprio l'incontro tra necessità delle persone e capacità delle istituzioni di sfruttare la tecnologia presente che nasce la smart city.

---

[4] Herman van den Bosch, "PlanIT Valley. The Smartest City Never Been Built", in *Smart City Hub*, 10 gennaio 2018, https://wp.me/p8qO7s-HN.

[5] Treccani, *Smart City*, http://www.treccani.it/vocabolario/smart-city_res-72b7b87c-89ec-11e8-a7cb-00271042e8d9_(Neologismi).

Una definizione più omnicomprensiva permette di racchiudere le tre componenti fondamentali, le istituzioni, i cittadini e le infrastrutture. In summa si può definire le smart city come "città dotate di capitale umano e istituzioni proattive, capaci di implementare infrastrutture digitali e analogiche che registrano dati in tempo reale, attraverso sensori, interconnettendo mondo fisico e mondo virtuale per il benessere dei cittadini".

Una smart city può quindi essere paragonata a un organismo umano, che possiede nelle infrastrutture, quindi nella tecnologia, i nervi connettori; nei sensori i sensi; e nella dimensione umana il cervello stesso e la creatività necessaria al funzionamento organico di tutte le altre parti.

6.2 Le componenti e le dimensioni delle smart city

Una volta definita l'essenza della smart city bisogna comprendere le sue componenti e dimensioni.

In primis, come sottolineato in precedenza, non può mancare la componente relativa al capitale umano, vero e proprio motore del progresso tecnologico. Città che hanno poli universitari capaci di svolgere ricerca e sviluppo di prototipi, amministrazioni comunali dotate di preparazione e competenza e altresì pronte a finanziare o ad attrarre finanziamenti in senso avveniristico e aziende proattive negli investimenti. Questo tipo di città sono anche definite *knowledge city*, *creative city* o *learning city*.

In seguito, l'infrastruttura gioca un ruolo chiave con la necessità di avere una dotazione hardware e software in grado di interconnettersi e informare decisore politico e cittadino sugli andamenti di determinati settori, da modificare per il primo o da sfruttare per il secondo. Si pensi per esempio alla densità di un determinato quartiere e al numero di persone che utilizzano l'auto privata o il trasporto pubblico in relazione al traffico generato da quello stesso quartiere. Tali caratteristiche rendono una città smart, *ubiquitous city*, in cui ogni cittadino può ottenere ciò di cui ha bisogno dappertutto, o una *information city*, in cui sia cittadini che amministratori hanno un accesso esteso alle informazioni attraverso il web o software appositi. È questo uno standard minimo per entrare nel novero delle città smart che ormai nel 2019 si sta raggiungendo in molte città europee ed italiane come la possibilità di accedere ai servizi della pubblica amministrazione anche da remoto senza doversi recare in uffici burocratizzati, o la possibilità di interagire online con gestori dei servizi di trasporto pubblico e consultare in tempo reale tempi di percorrenza.

Infine la sensoristica, importantissima sia per *policy* di lungo periodo che per riscontrare in tempo reale cambiamenti allo *status quo* della città o di un determinato quartiere. Il reperimento dei dati è il primo passaggio necessario per poter implementare un sistema di smart city. Avere sensori posizionati in punti nevralgici della città permette la raccolta dati e la successiva elaborazione di politiche sulla base di essi; in fase di progettazione di una smart city le amministrazioni possono optare per impiantistiche che privilegino una delle aree di possibile sfruttamento della tecnologia, siano esse l'ambiente, per misurare la qualità dell'aria, l'energia, per un efficientamento dei consumi e per evitare sovraccarichi a rete elettrica o sospensioni di flussi idrici, i trasporti, per velocizzare il traffico con ad esempio semafori intelligenti o sicurezza per il controllo di determinate aree a rischio. Altri dati vengono immessi nei sistemi attraverso sensori che appartengono ad aziende private, municipalizzate e non, che possono o meno condividerle con le amministrazioni delle città, sulla base di richieste o di contratti di servizio in cui questa condivisione è specificata.

La relazione tra tecnologia e società crea quindi una situazione simile alla teoria *actor-network*, dove la tecnologia diventa un abilitatore e partner nel realizzare i bisogni della società e migliorare la vita dei cittadini. La mancanza però di una validazione empirica dei framework proposti crea un gap tra accademia e professionisti, soprattutto per quanto riguarda gli utilizzi pratici della tecnologia nelle città.

La letteratura tende a classificare il termine smart, principalmente nel tentativo di condurre studi sul livello di avanzamento tecnologico di una città, in sei dimensioni: *smart people*, *smart economy*, *smart mobility*, *smart living*, *smart governance* e *smart environment*[6]. La tabella 1 propone degli indicatori utili a inquadrare le diverse possibilità offerte per il decisore politico dall'universo *smart*.

Essendo l'interesse di questo capitolo focalizzato sulla sicurezza nelle smart city si terrà in considerazione l'indicatore *smart policing and crime control* cercando di comprendere come tale indicatore è utilizzato nella geopolitica globale e come esso possa essere interpolato con indicatori di altre dimensioni.

[6] Arpan Kumar Kar et al., "Understanding Smart Cities: Inputs for Research and Practice", in Arpan Kumar Kar et al. (eds), *Advances in Smart Cities. Smarter People, Governance, and Solutions*, Boca Raton, CRC Press, 2017, p. 2.

Tabella 1 – Le sei dimensioni del termine "smart"

Smart people	Smart economy	Smart mobility	Smart living	Smart governance	Smart environment
• Higher education	• High-full time employment	• Local accessibility	• Better education	• Access to information	• Water resource management
• Social and ethnic diversity	• High economic productivity	• International accessibility	• Digital literacy programs	• Public utilities and services	• Smart energy management
• Openness and cohesion	• Entrepreneurs hip and globalization	• Green transportation systems	• Better health care	• Democratic participation	• Gas and particle pollution control
• Cosmopolitan outlook	• Idea and IP generation	• Public transportation	• Planned housing facilities	• Women participation	• Hazardous waste management
• Flexible approaches in work and life	• High-skilled labor and jobs	• Physical safety	• Cultural facilities	• Smart policing and crime control	• Solid waste management
• High work productivity	• Small supporting businesses	• Monitoring and control systems	• Sports facilities	• Urban planning support	• Sanitation management
• Entrepreneur focus and zeal	• Vocationally trained workforce	• Logistics and freight control	• Smart urban planning	• Grievance management	• Noise control
• Cultural plurality		• Commutation infrastructure	• ICT access	• Information security and risk management	
			• Low infant mortality		

Fonte: Arpan Kumar Kar et al., "Understanding Smart Cities: Inputs for Research and Practice", cit., p. 2.

6.3 CINA: LA PATRIA DELLA PERCEZIONE DEL CONTROLLO

Il tentativo di migliorare la sicurezza dei cittadini attraverso la tecnologia è notizia ben risaputa; in letteratura già dal secondo dopoguerra e nel mondo del cinema sin dagli anni '80 si sono proposti futuri distopici in cui la tecnologia svolgeva un ruolo di primo piano nella vita delle persone, basti pensare ai romanzi di Philip K. Dick o al film Matrix, etichettati come genere di fantascienza. Se la parola sorveglianza era il filo conduttore di tali narrazioni, nel 2019 ci troviamo di fronte a possibili differenti diramazioni di tale concetto. Sempre per rimanere nel mondo delle pellicole basti pensare al successo e ai possibili scenari distopici immaginati dalla serie tv di Netflix "Black Mirror". Se infatti ad oggi la tecnologia sembra aver raggiunto le narrative distopiche degli anni '80-'90, attraverso per esempio i software spia o i suggerimenti per gli acquisti basati sui nostri comportamenti online, i possibili futuri di *social ranking* o macchine della verità immaginate dalla filmografia recente non appaiono ancora del tutto praticabili nella realtà. Da un punto di vista geopolitico, comprendere in che direzione stanno virando le tecnologie messe in atto all'interno della

smart city può aiutarci a capire le strategie e le possibili implicazioni geopolitiche future sul tema.

Uno dei più importanti attori mondiali che sta sperimentando le nuove tecnologie applicandole alla smart city è la Cina. Con dieci città che superano i 10 milioni di abitanti, gli amministratori delle più grandi città cinesi puntano sulla tecnologia per facilitare i compiti delle forze di polizia. Negli ultimi anni i sistemi di controllo in sperimentazione e in esecuzione in alcune città sono saliti alla ribalta dei media, specialmente americani. La Cina sembra essere proiettata verso un sistema di ubiquità del controllo del cittadino. Oltre alla sorveglianza sui social network e ad un controllo capillare dell'infrastruttura di Internet, si rilevano sperimentazioni in atto su dispositivi mobili, siano esse telecamere o occhiali stile *google glasses* con tecnologie di riconoscimento facciale.

Già dal 2015 la polizia nazionale cinese e il ministero della Pubblica sicurezza avevano chiesto la creazione di una rete di videosorveglianza nazionale "onnipresente, completamente connessa, sempre attiva e completamente controllabile"[7]. Proteggere lo *status quo* del partito e del regime è una delle priorità del governo cinese. Per migliorare il controllo sui cittadini, specialmente nella turbolenta regione dello Xinjiang, la tecnologia è uno degli strumenti di supporto alle forze di sicurezza del Paese. Per quanto riguarda la minoranza Uiguri, sono ben noti i sistemi di controllo che la polizia cinese svolge sui social network e sulle telecomunicazioni nella regione[8]. Nel resto del Paese il programma cinese sembra essere più orientato a una lotta ai crimini comuni, come rintracciare e fermare individui accusati di corruzione, attraverso tecnologie di riconoscimento facciale, ma soprattutto a un progetto di *social scoring*, lanciato nel 2015 e, visto da una prospettiva europea, dai contorni decisamente inquietanti.

In Cina è anche in vigore una legge che controlla gli spostamenti ferroviari e aerei e telecamere di videosorveglianza con applicazioni di riconoscimento facciale e *checking* in tempo reale sono attive nelle maggiori stazioni e aeroporti cinesi. Per comprendere come un tale controllo capillare sia possibile, quindi come Pechino possa praticamente attuare tale

[7] Simone Pieranni, "Controllo e sicurezza. Gli occhi acuti della Cina", in *il manifesto*, 10 aprile 2019, https://ilmanifesto.it/controllo-e-sicurezza-gli-occhi-acuti-della-cina.

[8] Matt Rivers e Lily Lee, "Security Cameras and Barbed Wire: Living Amid Fear and Oppression in Xinjiang", in *CNN*, 9 maggio 2019, https://edition.cnn.com/2019/05/08/asia/uyghur-xinjiang-china-kashgar-intl/index.html.

sistema, occorre innanzitutto scindere il piano della ricerca storico-culturale da quella tecnologica.

Senza dover risalire al periodo della dinastia Song, in cui fu concepito il sistema *baojia*, dove diverse unità familiari si raccoglievano in chiave difensiva, si può ricordare che la rivoluzione cinese stessa è di tipo conservatore, se si permette l'ossimoro. L'idea alla base del partito comunista in Cina non era difatti di completa rottura con il passato, lo stravolgimento dell'ordine costituito non risultava come uno dei punti fondamentali e alcune tradizioni come il rapporto tra cittadino e stato centrale continuarono e seguitano ancora oggi sulla stessa linea.

Il controllo capillare attraverso la tecnologia quindi non si inserisce su una popolazione totalmente avulsa da pratiche di questo tipo, ma al contrario si instaura in una società in cui l'individuo si sente parte del tutto e contribuisce a mantenere l'ordine in opposizione al caos. L'avanzamento tecnologico si impone come supporto al mantenimento dell'ordine, risolvendo inefficienze burocratiche, ed è quindi per tale motivo alacremente supportato in Cina.

Così, si può leggere il sistema di *social credit* come una prosecuzione della tradizione di schedare i cittadini da parte dei quadri di partito attraverso il sistema *hukon*, in cui i dati personali già immagazzinati nei sistemi di partito sono digitalizzati e connessi con altri dati quali spostamenti, dati relativi ai conti bancari e conversazioni. Il *social scoring* esiste già a livello informale in Cina, ogni cittadino si sente parte della società e con essa, con il suo quartiere, la sua città, deve essere in armonia. Nel 2014 però il governo cinese ha annunciato un piano per costruire un sistema di crediti sociali nazionale da implementare entro il 2020[9]; per il momento tale sistema non è in funzione ma alcuni test sono stati attuati in diverse regioni e città cinesi. Il sistema dovrebbe essere una sorta di meccanismo di punizione e ricompense per migliorare il livello di fiducia e integrità dell'intera società cinese.

Da un punto di vista tecnologico gli investimenti del governo cinese nel settore informatico sono di vigore sin dal 2006, quando il governo cinese ha lanciato il National Medium- and Long-Term Program for Science and Technology Development, programma che destinava il 2,5 per cento minimo alla ricerca in campo tecnologico. In aggiunta, nel 2015 Xi Jinping ha lanciato il programma "Made in China 2025" per

[9] Celia Hatton, "China 'Social Credit': Beijing Sets Up Huge System", in *BBC News*, 26 ottobre 2015, https://www.bbc.com/news/world-asia-china-34592186.

rendere la Cina il primo Paese al mondo in dieci differenti settori manifatturieri tra cui la robotica e la tecnologia delle informazioni[10]. Non è un segreto nemmeno il forte investimento di Pechino nell'intelligenza artificiale (Ia); negli ultimi 12 mesi da una ricerca sul portale che raccoglie le informazioni su offerte di contratti pubblici in Cina, si evidenziano 847 progetti etichettati con "*xueliang gongcheng*", ovvero "occhi acuti", il programma governativo che mira a securitizzare le smart city attraverso l'uso massiccio della videosorveglianza con annessa Ia in cui il governo cinese ha investito 50 miliardi di yuan, circa 8 miliardi di euro[11].

Sarebbero circa 176 milioni le telecamere installate per motivi di sicurezza in Cina nel 2016, il numero più alto al mondo ma ancora relativamente modesto se relazionato al numero di abitanti. Gli Stati Uniti vantano 62 milioni di telecamere nel Paese su una popolazione totale di 372 milioni di abitanti, dunque una telecamera ogni 6 abitanti negli Usa e una ogni 8 abitanti in Cina[12].

È da sottolineare il vantaggio comparato di cui il governo di Pechino gode in confronto ai suoi competitor democratici, derivante dal fatto di poter dirigere e pianificare in modo verticale l'innovazione nel Paese e dalla possibilità di poter disporre di una massiccia forza lavoro. La Cina difatti, attraverso l'approccio dirigista, raggiunge economie di scala nel comparto tecnologico difficilmente attuabili da governi democratici.

Se l'Ia guiderà un nuovo boom economico cinese non è ancora chiaro. Ciò che è ben noto invece è che l'Ia necessità di una grande mole di dati per raggiungere un livello accettabile di funzionamento e di certezza dei risultati. Nel campo della sicurezza le autorità cinesi non hanno problemi a reperire i dati da un punto di vista tecnico, è tuttavia la gestione del dato che risulta problematica. Una mole enorme di dati va analizzata e utilizzata per alimentare i processi di *learning* del dispositivo o della piattaforma di gestione del dato. Per fare un esempio pratico i nuovi

[10] Lorenzo Mariani, "La geopolitica del 5G e lo scontro Usa-Cina", in *Focus euroatlantico*, n. 11 (gennaio-marzo 2019), p. 26, https://www.iai.it/it/node/10273.

[11] Nina Xiang, "Chinese Unicorn Terminus Combines AI and IoT to Empower Smarter Cities", in *Forbes*, 5 marzo 2019, https://www.forbes.com/sites/ninaxiang/2019/03/05/chinese-unicorn-terminus-combines-ai-and-iot-to-empower-smarter-cities.

[12] Sul tema della videosorveglianza si veda: Paul Mozur, Jonah M. Kessel e Melissa Chan, "Made in China, Exported to the World: The Surveillance State", in *The New York Times*, 24 aprile 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

occhiali in dotazione alla polizia di Pechino[13] possono associare un individuo ad un *database* di 10.000 volti, cercando il *matching*. È chiaro che più ampio diventa il campione più tempo occorrerà e più difficile sarà avere un rapido riscontro. Tuttavia, la consapevolezza all'interno della popolazione dell'esistenza di un sistema simile genera una deterrenza calcolata, con conseguenti ricadute positive per la diminuzione del livello di criminalità; è così che se per funzionare un *panopticon* può anche essere semplicemente prospettato, allo stesso modo si possono ridurre i crimini in determinate aree dove si ha la percezione di essere controllati. La versione cinese dell'uso della tecnologia può quindi ovviare a problemi tecnici sia attraverso la ricerca, sia attraverso la sola percezione del controllo.

6.4 Stati Uniti: tra innovazione e "techlash"

Diversamente dalla Cina, gli Stati Uniti appaiono in seria difficoltà per quanto riguarda l'utilizzo della tecnologia in ambito di sicurezza.

Gli scandali dell'Nsa e di Cambridge Analytica negli ultimi anni hanno minato la credibilità delle autorità statunitensi e generato nell'opinione pubblica un forte senso di opposizione allo sviluppo di tecnologie in generale e nello specifico ambito della sicurezza.

Il lemma "*techlash*" è stato inserito dal Financial Times nel novero delle parole chiave del 2018 non a caso[14]. Con questo termine, traducibile con "frustata tecnologica", la stampa statunitense vuole sottolineare una sorta di risacca dell'ondata digitale che sta vivendo la comunità americana. Una controcultura nata nella stessa Silicon Valley che si oppone ad una tecnologia invasiva che permea tutti gli aspetti della vita umana. Il fatto che il termine nasca proprio nella culla della tecnologia ha una forte valenza simbolica, in quanto segnala come chi si sta occupando di nuove tecnologie si stia iniziando ad accorgere che il loro utilizzo non sempre porta giovamento e che la messa in sicurezza di un numero enorme di dati e servizi non sempre è possibile. Il termine è stato coniato

[13] Josh Chin, "Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal", in *The Wall Street Journal*, 7 febbraio 2018, https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353.

[14] Rana Foroohar, "Year in a Word: Techlash", in *Financial Times*, 16 dicembre 2018, https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e.

dall'Economist già nel 2013[15], ed è stato rilanciato a seguito dei recenti crolli in borsa dei giganti hi-tech come Facebook e Google. Nel complesso, il biennio 2018-2019 è stato molto difficoltoso per le compagnie tecnologiche negli Stati Uniti che hanno dovuto affrontare il tentativo dell'amministrazione Trump di andare verso un maggiore controllo di tipo statale sul comparto tecnologico, e soprattutto di porre limiti al libero mercato e alle imprese straniere (principalmente cinesi) per motivi di sicurezza nazionale.

Tutto ciò rischia di avere una ricaduta notevole anche per le imprese che lavorano nel settore della sicurezza delle smart city. Negli Stati Uniti è il settore privato a trainare il pubblico nella corsa all'innovazione tecnologica. Sebbene non bisogna né dimenticarsi né sottovalutare il ruolo del Darpa per il progresso tecnologico degli anni '70-'80, è evidente che la diversa impostazione del *laissez-faire* americano negli anni '90 ha portato una corsa all'oro tecnologico che è in questi anni ad un bivio. Il modello storico-culturale degli Stati Uniti, un liberalismo dilagante evoluzione dell'umanesimo e della rivoluzione industriale, applicato alla tecnologia ha funzionato fin quando non ci si è accorti che i dati, tanto esaltati come nuovo petrolio del ventunesimo secolo, possono contenere anche particelle tossiche e diventare un'arma facilmente spendibile nel contesto internazionale, siano esse e-mail scottanti o tentativi di influenzare le elezioni politiche attraverso i social media.

Presenza di una controcultura che è ben visibile, per ritornare al tema della sicurezza nelle smart city, nella decisione dello scorso maggio della città San Francisco di mettere al bando le tecnologie di riconoscimento facciale nella città. Il consiglio dei supervisori, organo legislativo della contea e della città di San Francisco ha infatti emanato lo scorso 14 maggio un'ordinanza per fermare la "sorveglianza segreta" delle forze di polizia affermando che per raggiungere la sicurezza non serve vivere in uno stato di polizia[16]. L'ordinanza copre un vasto ventaglio di soluzioni tecnologiche di supporto alle forze di polizie che variano dai lettori ottici di targhe delle automobili ai sensori di rilevazione degli spari. È un passo indietro nel progresso tecnologico importante quello deciso dalla città di San Francisco che si scontra con altre realtà americane come Boston, la quale ha al

[15] Adrian Wooldridge, "The Coming Tech-Lash", in *The Economist*, 18 novembre 2013, https://www.economist.com/news/2013/11/18/the-coming-tech-lash.

[16] Khari Johnson, "San Francisco Supervisors Vote to Ban Facial Recognition Software", in *VentureBeat*, 14 maggio 2019, https://wp.me/p8wLEc-aszH.

contrario un dipartimento di polizia talmente orientato all'utilizzo della tecnologia da avere una pagina online dedicata alle donazioni dei privati[17].

A differenza della Cina, negli Stati Uniti l'innovazione proviene quindi dalle imprese, sia grandi che piccole. Anche in questo caso gli obiettivi tecnologici si fondano su concezioni storico-culturali ben radicate. La storia degli Stati Uniti ha sempre visto la necessità di porre l'individuo al centro dei ragionamenti filosofici e soprattutto libero da imposizioni; se con la rivoluzione americana gli Stati Uniti si sono liberati dal giogo inglese, il cittadino statunitense è sì partecipe dello Stato e parte dello stesso ma non deve percepirlo come troppo invadente negli affari privati. È così che l'innovazione, anche nel campo tecnologico securitario, parte dai privati, siano esse piccole o grandi aziende che propongono nuovi prodotti alle polizie locali da un lato e al Federal Bureau of Investigation (Fbi) dall'altro. Molto interessante è notare quindi la varietà di prodotti sulla quale si basa il sistema di sicurezza americano. L'Ia sembra essere appannaggio del livello federale, con l'Fbi impegnata nel difendere il suo operato da interrogazioni parlamentari, mentre le diverse città operano con il supporto di imprese private.

In alcune città come Boston, Chicago e Miami sono in fase di sperimentazione sistemi di sensoristica avanzata per il riconoscimento dei colpi di arma da fuoco. Tali sensori, installati in diversi punti nevralgici della città ed alimentati attraverso processi di *machine learning*, forniscono un *alert* in tempo reale alle forze dell'ordine sui luoghi in cui è in corso un conflitto a fuoco. In funzione in alcune città già dal 2007, appaiono essere sistemi di supporto efficienti ma anche costosi, sia in termini di investimento iniziale che per l'eventuale sostituzione e alimentazione[18].

Sembrano invece arrancare le tecniche di polizia predittiva (*preventing policing*), giudicata dal Time come una delle migliori 50 invenzioni del 2011 e basata sull'interpolazione tra dati e algoritmi[19]. I software di polizia predittiva si fondano infatti sull'elaborazione di dati relativi a indagini passate[20]. Il sistema processa dati di crimini avvenuti in passato per tentare

[17] Boston Police Foundation Website, "New Technology", https://bostonpolicefoundation.org/new-technology.

[18] La lista delle città in cui l'azienda Shotspotter ha installato i sensori di rilevamento di spari è disponibile online: https://www.shotspotter.com/cities.

[19] Lev Grossman et al., "The 50 Best Inventions", in *Time*, 28 novembre 2011; Jackie Wang, "'This Is a Story About Nerds and Cops': PredPol and Algorithmic Policing", in *e-flux*, n. 87 (dicembre 2017), https://www.e-flux.com/journal/87/169043/this-is-a-story-about-nerds-and-cops-predpol-and-algorithmic-policing.

[20] Adam Mann, "How Science Is Helping Stop Crime Before It Occurs", in *NBC News*, 6

di predire o meglio di evidenziare possibili aree in cui avverranno crimini simili in futuro. Il ragionamento di base è molto semplice e funzionale, se un quartiere della città ha un'alta casistica di effrazioni in luoghi privati, significa che tale possibilità si può ricreare nel futuro. Tale tecnologia è stata utilizzata per periodi di prova da diversi dipartimenti di polizia locali, come quelli di Boston, Los Angeles e Santa Cruz. Malgrado le potenzialità descritte, questa tecnologia è stata accusata di aumentare i pregiudizi razziali[21] e ghettizzare aree della città, rischiando di creare "profezie autoavveranti"[22].

Infine molto abbondante appare il mercato dei droni. Secondo il Center for the Study of the Drone sono 910 le agenzie pubbliche statunitensi in possesso di droni, delle quali 580 si occupano di sicurezza (e non solo di *safety*)[23]. Una mole di prodotti di vario genere e numero, non coordinati a livello centrale, che ha diversi utilizzi, dalla sorveglianza al *tracking* di persone, a seconda del tipo di modello. Anche per questa innovazione alcuni stati hanno però iniziato a regolamentare e controllare l'operato delle singole polizie: è il caso di Florida, Maine, Virginia e Nord Dakota che prevedono la richiesta di un mandato per poter operare o del Rhode Island che sta discutendo un bando integrale alla tecnologia[24].

Un grande provider intenzionato a sperimentare la tecnologia di riconoscimento facciale e a cooperare con le forze di polizia è Amazon. Il gigante dell'e-commerce ha lanciato un nuovo programma chiamato Rekognition che strizza l'occhio alle forze dell'ordine invitandole con un post sul proprio blog a utilizzare l'algoritmo alla base della tecnologia (su basi legali non chiare) per migliorare il lavoro di riconoscimento in indagini aperte[25]. È una tecnologia di riconoscimento facciale molto simile a quella utilizzata da Facebook per permettere di taggare

---

ottobre 2017, https://www.nbcnews.com/mach/science/how-science-helping-stop-crime-it-occurs-ncna805176.

[21] Sylvia Thomson, "'Predictive Policing': Law Enforcement Revolution or Just New Spin on Old Biases? Depends Who You Ask", in *CBC News*, 24 settembre 2018, https://www.cbc.ca/amp/1.4826030.

[22] Kristian Lum, "Limitations of Mitigating Judicial Bias with Machine Learning", in *Nature Human Behaviour*, 26 giugno 2017.

[23] Dan Gettinger, "Public Safety Drones: An Update", in *Center for the Study of the Drone Datasheets*, maggio 2018, https://dronecenter.bard.edu/public-safety-drones-update.

[24] Ibid.

[25] Chris Adzima, "Using Amazon Rekognition to Identify Persons of Interest for Law Enforcement", in *AWS Machine Learning Blog*, 15 giugno 2017, https://aws.amazon.com/blogs/machine-learning/using-amazon-rekognition-to-identify-persons-of-interest-for-law-enforcement.

in automatico un amico in una foto del famoso social network. In aggiunta, è di poche settimane orsono la notizia di una nuova configurazione programmabile con il sistema Alexa che permetterebbe all'utente di segnalare la sua uscita e di collegare eventuali rumori ascoltati dal sistema alla stazione di polizia più vicina per permettere un tempestivo intervento in caso di effrazione[26]. Sono progetti in fase molto embrionale, i quali se da un lato dimostrano il livello di tecnologia a cui un utente può avere accesso con poche centinaia di euro, dall'altro sono soggetti al rischio di falsi positivi e di intasare le stazioni di polizia in caso tali apparecchi funzionassero in modo totalmente automatico. Ciononostante è pur vero che i sistemi di allarme collegati alle stazioni di polizia funzionano al momento in modo analogo, con l'unica differenza che utilizzano sensori di movimento e non acustici, ed è altrettanto vero che sistemi come Alexa sono già stati utilizzati come prova per casi di omicidio[27].

Per quanto riguarda l'uso dell'Ia è, come sottolineato, l'Fbi a gestire *in primis* l'innovazione. Recentemente, il 4 giugno 2019, il Committee on Oversight and Reform del Congresso ha svolto un'audizione sul sistema di sorveglianza dell'Fbi impiegante l'Ia in risposta ai dubbi sull'utilizzo dei database statali e federali[28]. La relazione del vice-direttore dell'Fbi, Kimberly Del Greco, illustra l'approccio americano a questa tecnologia. L'Fbi, sostiene Del Greco, ha come necessità critica di costruire un rapporto di fiducia con il cittadino; per garantire il rispetto delle libertà civili, parte fondante della cultura americana, sono previsti una serie di meccanismi di controllo e supervisione. L'uso dell'Ia da parte dell'Fbi viene regolato a livello di *policy* su base semestrale da un Advisory Policy Board composto da 111 attori (a livello locale e federale parte), diversi audit sono completati da agenzie interne ed esterne all'Fbi e dal dicembre 2017 ogni operatore di sicurezza impegnato nel programma di Ia svolge un addestramen-

[26] Michael Brown, "Amazon's Alexa Guard Adds New Security Features to Amazon Echo Smart Speakers", in *TechHive*, 14 maggio 2019, https://www.techhive.com/article/3395496.

[27] Elliott C. McLaughlin, "Suspect OKs Amazon to Hand Over Echo Recordings in Murder Case", in *CNN*, 26 aprile 2017, https://edition.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html.

[28] US House Committee on Oversight and Reform, *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*, 4 giugno 2019, https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-ii-ensuring-transparency-in-government-use.

to specifico in tema di privacy e libertà civili[29]. Infine da un punto di vista tecnico, ogni anno l'Istituto nazionale per gli Standard tecnologici, apparato statale del Dipartimento dell'Economia svolge test sulla piattaforma.

L'Fbi, attraverso la Criminal Justice Information Services Division utilizza due sistemi di riconoscimento facciale, il sistema Next Generation Identification (Ngi) e il Facial Analysis, Comparison, and Evaluation (Face) Services Unit. Il sistema Ngi collega le richieste provenienti da personale di polizia autorizzato con l'Interstate Photo System, un database su scala nazionale che attraverso l'utilizzo dell'Ia risponde alle richieste con una galleria di massimo 50 foto che possono corrispondere al soggetto, le quali vengono poi selezionate "manualmente" dall'operatore per il confronto finale. Il sistema ha registrato dal 2017 ad aprile 2019 un totale di 152.565 richieste di accesso, circa 200 richieste al giorno[30]. Il Face ha una struttura molto simile ma è ristretto a casi trattati dall'Fbi stessa. L'unità nel solo 2018 ha registrato 390.186 ricerche su vari database, per un totale di più di 1.000 al giorno[31]. Il sistema sembrerebbe quindi solo un ampliamento in termini di ampiezza del campione del vecchio metodo del confronto all'americana, con telecamere al posto dei testimoni, che renderebbe meno soggetto a pregiudizi e più oggettivo il riconoscimento. Ciò che maggiormente differenzia, e altresì preoccupa i difensori dei diritti civili, sono la popolazione con cui sono alimentati i due sistemi. Nel Ngi il dato proviene da un sistema comparabile al Sistema di Informazione d'Indagine in dotazione alle forze di sicurezza italiane, in cui sono schedati tutti coloro che hanno commesso un crimine. Ben diversa, tuttavia, è la quantità di database da cui pesca il Face, in quanto il sistema reperisce i dati dai passaporti di tutti i cittadini che risiedono o transitano negli Stati Uniti, unitamente e a quelli accumulati dalle richieste di visto e patenti di guida[32]. Il sistema centrale americano quindi viaggia su un doppio binario, e seppur tutelato da diverse procedure e test risulta distante dalla cultura europea di tutela delle libertà civili.

[29] Kimberly J. Del Greco, *Statement Before the Committee on Oversight and Reform*, 4 giugno 2019, http://docs.house.gov/meetings/GO/GO00/20190604/109578/HHRG-116-GO00-Wstate-DelGrecoK-20190604.pdf.

[30] Ibid., p. 3.

[31] Ibid., p. 4.

[32] Ibid.

6.5 Europa: verso una securitizzazione delle smart city?

E in Europa? Il contesto europeo parte da una concezione delle smart city molto frammentata e che combina le fondamenta dello stato di diritto con una visione fortemente garantista, con l'anima "verde" europea e la atomizzazione del mercato. L'Ue ha lanciato molti progetti all'interno del programma Horizon 2020, il più grande fondo europeo esistente dedicato alla ricerca in ambito di innovazione tecnologica. Dal 2013 al 2019 ben 58 progetti includono il termine smart city e prevedono un budget medio di 5 milioni di euro ciascuno. Partendo dai titoli dei progetti è possibile operare una suddivisione tematica e temporale per tracciare un *fil rouge* sulla strategia di ricerca dell'Ue. Oltre a progetti che coprono temi più generali riferiti all'innovazione (25), come quelli dedicati a un miglioramento degli stili di vita, si nota un interesse specifico per il settore energetico, la gestione dei rifiuti e l'ambiente (25) e una piccola nicchia per trasporti (8), patrimonio culturale (5) e sicurezza (5)[33]. La distribuzione dei temi dei progetti mostra una predisposizione europea verso il concetto di smart city come una città "verde" e vivibile, ma è proprio il tema della sicurezza, quello su cui l'Ue sta investendo maggiormente negli ultimi anni, senza calcolare la mole di progetti finanziati dal Fondo Sicurezza interna della Direzione generale Migrazione e Affari interni della Commissione europea. Tale proliferazione di iniziative evidenzia chiaramente l'interesse specifico nel settore dell'innovazione della sicurezza. Solo per fare un esempio, l'ultimo progetto messo a bando intende migliorare le capacità di risposta degli operatori di pubblica sicurezza all'interno degli spazi pubblici cittadini grazie all'apporto tecnologico.

D'altro canto, sempre a livello europeo le forti strette in ambito di scambio e gestione dei dati, provenienti dal nuovo Gdpr e dalla Direttiva Nis palesano la cultura garantista e fortemente protettrice delle libertà individuali presente in Europa. Se si aggiunge a questo discorso il clamore suscitato nell'opinione pubblica dalle rivelazioni di WikiLeaks prima e della sorveglianza dell'Nsa americana dopo, si può immaginare quanto sarà difficile una piena penetrazione a livello statale di tali tecnologie.

[33] I dati sono tratti dal portale Cordis dell'Unione europea che contiene tutti i progetti finanziati attraverso fondi europei.

Chi traina l'innovazione tecnologica in Europa nel supporto alle forze di polizia in una smart city sono, similmente al caso americano, le imprese. Anche in Europa si stanno sviluppando aziende capaci di fornire strumenti predittivi, software e hardware alle forze di polizia ma, come negli Stati Uniti, la legislazione sta controllando l'avanzamento e la mancanza di risorse finanziarie e di personale impedisce una veloce implementazione di tali tecnologie.

L'Inghilterra è stata la prima a dotare i *bobbies* di strumenti tecnologici di *predictive policing* e anche la prima in Europa a cancellare il programma. Al momento 11 città usano questo tipo di software a supporto delle forze di polizia nonostante le forti critiche delle associazioni di diritti civili, che le accusano di aumentare i pregiudizi razziali e verso le minoranze[34]. In particolare la città di Kent ha abbandonato il progetto vista la difficoltà di dimostrare la profittabilità dell'investimento a causa dell'elevato costo della tecnologia, che si aggirava intorno alle 100.000 sterline annue, a fronte di un modesto utilizzo. Anche il mondo dei droni è in fase di sperimentazione in Inghilterra: molte polizie locali investono nel loro utilizzo nonostante vi siano lacune giuridiche, ma il risparmio in confronto all'utilizzo degli elicotteri è evidentissimo con costi che si aggirano intorno alle 5.000 sterline per un drone contro le 100.000 di un elicottero. Anche in Inghilterra manca un approccio statale a tale tema e la dimostrazione è la totale assenza della dimensione della sicurezza nel progetto governativo relativo al futuro delle smart city concluso nel 2016[35].

In Germania la competenza dell'innovazione tecnologica è delegata principalmente alle polizie federali. Sin dal 2014 ben sei stati federali su 14 hanno iniziato a sperimentare software di polizia predittiva e anche in questo caso appare evidente la frammentazione del mercato dovuta a una mancanza di pianificazione a livello centrale: sono ben cinque le società che forniscono servizi ai sei stati tedeschi. È interessante anche notare l'interesse dell'accademia all'efficienza di tali sistemi, assente negli Stati Uniti, sebbene la ricerca non abbia prodotto evidenze a favore dell'utilizzo della tecnologia. Anche in questo caso sono stati infatti osservati fenomeni di *bias* e il rischio di mancato efficientamento dei tempi degli

[34] Frances Perraudin, "Facial Recognition Must Not Introduce Gender or Racial Bias, Police Told", in *The Guardian*, 29 maggio 2019, https://gu.com/p/bt6q9.

[35] UK Government, *Future of Cities*, 2013-2016, https://www.gov.uk/government/collections/future-of-cities.

operatori di polizia[36]. In aggiunta va notato che non sono previsti scambi di dati automatizzati tra polizia e amministrazione pubblica e viceversa, venendo così a mancare una delle componenti chiave del processo di securitizzazione della smart city[37].

Infine in Italia la Polizia di Stato ha iniziato a utilizzare dal 2018 il Sistema automatico di riconoscimento immagini (Sari)[38], un software che consente di comparare le immagini provenienti da telecamere di sicurezza con le immagini presenti nel database del Sistema automatizzato di identificazione delle impronte (*Automatic Fingerprint Identification System*, Afis)[39] che contiene sedici milioni di cartellini fotosegnaletici redatti da Polizia di Stato, Carabinieri, Guardia di Finanza e altre polizie estere con il supporto di Interpol e dell'Eurodac, il database europeo dei richiedenti asilo[40]. Il primo caso di utilizzo nel luglio 2018[41], aveva destato scalpore nell'opinione pubblica italiana, visto il copioso numero di dati contenuti nel database[42] al punto da portare a un'interrogazione parlamentare il cui iter è ancora in corso[43]. Non è nota la frequenza con cui la Polizia di Stato utilizzi tale software né altri dati tecnici come la percentuale di attendibilità e quali siano i database consultati: motivo per il quale probabilmente il sistema non è al momento utilizzato alla massima potenzialità, nonostante l'efficacia dimostrata nei casi noti[44].

---

[36] Kai Seidensticker, Felix Bode e Florian Stoffel, "Predictive Policing in Germany", in *KOPS Papers*, agosto 2018, https://kops.uni-konstanz.de/handle/123456789/43114.

[37] Dominik Gerstner, "Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg", in *European Journal for Security Research*, vol. 3, n. 2 (ottobre 2018), p. 115-138.

[38] Si vedano i documenti allegati al bando di gara per la fornitura della soluzione integrata per il Sari: https://www.poliziadistato.it/articolo/15557c52775a3724103220539. Un video di presentazione è disponibile in YouTube: https://youtu.be/rAme2IgBxqw.

[39] Polizia di Stato, *Dalle impronte alle foto segnaletiche*, 11 gennaio 2008, https://poliziadistato.it/articolo/1226.

[40] Parlamento europeo, *Asylum: Deal to Update EU Fingerprinting Database*, 19 giugno 2018, http://www.europarl.europa.eu/news/en/press-room/20180618IPR06025.

[41] Donatella Fioroni, "Brescia: ladri d'appartamento scoperti grazie al riconoscimento facciale", in *Notizie Polizia di Stato*, 7 settembre 2018, https://www.poliziadistato.it/articolo/135b92536bb3957899899171.

[42] Raffaele Angius e Riccardo Coluccini, "Riconoscimento facciale, nel database di Sari quasi 8 schedati su 10 sono stranieri", in *Wired*, 3 aprile 2019, https://www.wired.it/?p=240946.

[43] Atto Camera: Interrogazione a risposta scritta 4/01149, 19 settembre 2018, http://aic.camera.it/aic/scheda.html?numero=4/01149&ramo=CAMERA&leg=18.

[44] Polizia di Stato, *SARI = Sistema Riconoscimento Automatico Immagini. La Polizia di Stato ad Arezzo individua e denuncia i primi 7 ladri*, 4 ottobre 2018, https://questure.poliziadistato.it/it/Arezzo/articolo/10945bb6148a60216596783584.

Dall'esperienza di un singolo, l'ex assistente capo della Polizia di Stato Mario Venturi, anche in Italia è stato sviluppato un software di polizia predittiva. Volto a migliorare le prestazioni del software utilizzato dai colleghi statunitensi e tedeschi, tale software non adotta un approccio *hot-spot* ma prevede invece l'utilizzo dei dati per migliorare le analisi riguardanti la serialità dei casi[45]. Non un utilizzo quantitativo dei dati quindi ma un approccio più qualitativo e "vecchio stile" che predilige la componente umana a quella tecnologica. Il software immagazzina fino a 11mila variabili per ogni reato, come arma del delitto, colore degli abiti o tecnica utilizzata, creando delle serialità che vengono poi analizzate dagli operatori di polizia[46].

Infine da segnalare l'esperienza del progetto E-Security, finanziato dalla Direzione generale Migrazione e Affari interni della Commissione e implementato tra il 2013 e il 2016 a Trento[47]. In questo caso il tema della sicurezza urbana predittiva è stato interconnesso alle potenzialità della smart city, con la prima esperienza europea di un team che includeva operatori di sicurezza (Polizia di Trento), ricerca scientifica (Fondazione Bruno Kessler) e amministrazione pubblica (Comune di Trento). Il progetto ha incrociato database della città e delle forze di polizia per cercare di comprendere non solo il momento e il luogo in cui si verificano i crimini ma anche le motivazioni sottostanti ad essi. Gli indicatori creati hanno quindi tenuto conto anche di concetti come vittimizzazione, insicurezza dei cittadini e disordine urbano per intercettare correlazioni tra crimini e ambiente e migliorare la percezione di sicurezza e l'efficienza delle forze di polizia.

Conclusioni

L'analisi delle diverse esperienze internazionali nell'utilizzo della tecnologia per migliorare la sicurezza in una smart city ha messo in mostra le

[45] Gianni Santucci, "Milano, il programma anti rapine diventa una startup della sicurezza", in *Corriere della Sera*, 10 aprile 2018, https://milano.corriere.it/notizie/cronaca/18_aprile_10/milano-programma-anti-rapine-diventa-startup-sicurezza-a355ba22-3c81-11e8-87b2-a646d975b0f5.shtml.

[46] Andrea Daniele Signorelli, "Il software italiano che ha cambiato il mondo della polizia predittiva", in *Wired*, 18 maggio 2019, https://www.wired.it/?p=244851.

[47] Andrea Di Nicola et al., *eSecurity e le nuove frontiere della sicurezza urbana. Un sistema informativo per forze dell'ordine e amministrazioni locali*, Università degli Studi di Trento, 2015, http://www.ecrime.unitn.it/index.php?option=com_content&view=article&id=439.

molteplici vie percorribili e i diversi approcci geopolitici basati su altrettante differenti esperienze storiche. Dall'analisi si evince come nonostante sia evidente che la rivoluzione tecnologica ha definitivamente invaso il campo della sicurezza urbana, sembra mancare un approccio comune da parte delle autorità, per lo meno nazionali, nel concepirne i possibili utilizzi ma anche i limiti.

Non accompagnando il progresso tecnologico con un chiaro disegno politico si rischia non solo un eccessivo e intrusivo utilizzo della tecnologia per garantire la sicurezza ma anche di non cogliere le opportunità offerte da tale tecnologia. Attualmente è già molto difficile raggiungere un ottimo paretiano condivisibile da tutta l'opinione pubblica nella bilancia tra sicurezza e libertà individuali, l'aggiunta della tecnologia rende tale bilancia ancora più instabile e solo un effettivo controllo dei decisori politici può garantire che entrambi i temi siano soppesati.

Ciò che non va mai sottovalutato inoltre, specialmente in un ambito sensibile come la sicurezza dei cittadini, è che la tecnologia deve rimanere sempre un supporto alle azioni umane e non deve travalicare il ruolo del personale specializzato. Per migliorare la sicurezza nelle metropoli sempre più in espansione è fondamentale, infine, un maggiore dialogo tra gli operatori pubblici, municipalità e forze di polizia, gli attori privati fornitori dei servizi e i luoghi di formazione del sapere, università e centri di ricerca. Dialogo necessario nella fase di progettazione delle innovazioni per il cittadino per rendere quell'organismo, chiamato smart city, totalmente funzionale ai bisogni dei cittadini.

7.
Investimenti intangibili, concentrazione dei mercati e implicazioni politiche

Nicola Bilotta

Le multinazionali di Internet hanno anche più potere perché non solo creano e vendono prodotti, ma forniscono e delineano le infrastrutture digitali dalle quali i cittadini dipendono sempre di più.
Rebecca MacKinnon

L'ascesa nell'economia degli intangibili rappresenta un punto di rottura storico nelle dinamiche strutturali del capitalismo contemporaneo. La ricchezza globale non è più solamente prodotta dalle fabbriche e dal capitale finanziario ma è sempre di più il risultato di una catena del valore basata su beni e attività de-materializzate. Questa transizione è accelerata in maniera radicale dalla digitalizzazione dei processi produttivi che grazie allo sfruttamento delle tecnologie stanno incrementando la propria efficienza e – potenzialmente – la propria redditività.

Questa rapida trasformazione ha dei chiari effetti sulle dinamiche di mercato. La proprietà del capitale intangibile può facilitare l'emersione di mercati altamente concentrati in cui un numero limitato di attori privati potrebbe imporsi nell'economia globale sfruttando una superiore capacità innovativa, produttiva e di redditività. Oltre a ciò, bisogna tenere in considerazione che la globalizzazione viene potenziata dall'avanzamento tecnologico e dalla digitalizzazione favorendo il consolidamento di attori privati transnazionali.

In una realtà in cui l'economia è strutturata da regole nazionali e sovranazionali, questi cambiamenti degli equilibri industriali hanno anche degli effetti non trascurabili sui supposti condizionamenti tra poteri economici privati e istituzioni rappresentative su varia scala (locale, nazio-

nale e sovranazionale). Come ricordato dal premio Nobel all'economia Joseph Stiglitz, i processi di accentramento del potere economico si riflettono anche su un concentramento del potere politico con gravi implicazioni sociali, politiche ed economiche[1].

Le nuove dinamiche di mercato legate alla digitalizzazione dell'economia non sono di per sé né negative né positive. Contestualizzarne i trend e le implicazioni diviene una sfida cruciale per cercare di mitigarne gli effetti negativi e potenziarne quelli positivi.

7.1 Gli intangibili

Gli asset intangibili sono definibili come quelle risorse e patrimoni non incorporati in beni fisici o in attività finanziarie. Essi possono essere categorizzati in due macro aree principali: quelli determinati dalla proprietà intellettuale – come il brand, i brevetti, il copyright etc. – e quelli competitivi – tra cui il capitale umano, la capacità produttiva, i software o le piattaforme digitali[2]. Gli intangibili non sono un prodotto della storia umana più recente, hanno sempre fatto parte dello sviluppo della società. Dietro la creazione della ruota o del telaio, c'erano idee. Ciò che rappresenta un potenziale cambiamento è la sempre più crescente importanza degli intangibili nell'economia e il loro potenziale impatto sulla produttività, sulla crescita e sull'innovazione globale.

Nel 2013 per ogni dollaro investito in beni tangibili nelle economie sviluppate 1,1 dollari sono stati allocati in intangibili[3]. I flussi di investimenti – insieme alla forza lavoro – vengono considerati nelle maggiori teorie economiche un fattore produttivo chiave per stimolare la crescita. Per questo motivo, la transizione da un'economia basata su investimenti tangibili ad una intangibile diviene di cruciale importanza perché ridisegna potenzialmente le dinamiche e gli effetti dei meccanismi di mercato.

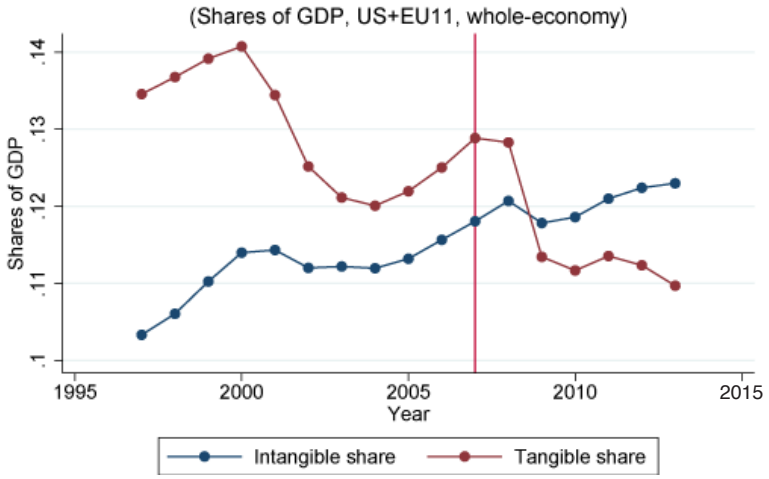
---

[1] Joseph Stiglitz, "Inequality, Stagnation, and Market Power. The Need for a New Progressive Era", in *Roosevelt Institute Working Papers*, novembre 2017, https://rooseveltinstitute.org/?p=25866.

[2] Sandrine Labory, "Intangibile", in *Dizionario di Economia e Finanza*, Treccani, 2012, http://www.treccani.it//enciclopedia/intangibile_(Dizionario-di-Economia-e-Finanza).

[3] Jonathan Haskel e Stian Westlake, *Capitalismo senza capitale. L'ascesa dell'economia intangibile*, Milano, Franco Angeli, 2018.

Figura 8 – Percentuale di investimenti tangibili e intangibili in rapporto al Pil negli Stati Uniti e in 11 stati Ue



Fonte: Jonathan Haskel e Stian Westlake, "Productivity and Secular Stagnation in the Intangible Economy", in *Vox*, 31 maggio 2018, https://voxeu.org/node/62502.

Questo cambiamento è riscontrabile anche nel mercato azionario. Osservando le S&P 500[4], è stato calcolato che circa l'80 per cento del loro valore consiste in asset intangibili. Amazon, Alphabet, Facebook e Microsoft hanno una capitalizzazione di circa 4,4 trilioni di dollari ma il valore dei loro asset tangibili sarebbe solamente circa il 5 per cento di questa cifra[5]. Secondo l'annuale studio di Brand Finance, il valore degli asset intangibili delle prime cento multinazionali al mondo ammonterebbe a quasi 50 trilioni di dollari con Amazon (827 miliardi), Microsoft (686 miliardi), Apple (648 miliardi), Alphabet (576 miliardi) e Alibaba (478 miliardi) a guidare la classifica[6].

Le conseguenze strutturali di questa evoluzione sull'economia globale sono strettamente legate alle caratteristiche intrinseche dei beni intangibili che per loro natura tendono ad avere differenti proprietà rispetto alle

[4] Il S&P 500 è un indice che rappresenta le 500 aziende a più alta capitalizzazione nella borsa di New York.

[5] Trevor Little, "Amazon Overtakes Microsoft to Top Intangible Value Ranking; Research Calls for 'Revolution' in Accounting", in *World Trademark Review*, 17 ottobre 2018, https://www.worldtrademarkreview.com/brand-management/amazon-overtakes-microsoft-top-intangible-value-ranking-research-calls.

[6] Brand Finance, *Global Intangible Finance Tracker (GIFT™) 2018*, ottobre 2018, https://brandfinance.com/knowledge-centre/market-research/global-intangible-finance-tracker-gift-20181.

risorse tangibili. Le risorse intangibili tendono ad avere alti costi iniziali e bassi costi di riproduzione, rendendo le loro attività facilmente scalabili. Queste due caratteristiche fanno sì che gli asset intangibili abbiano alti costi sommersi ("*sunk cost*") che rendono questi investimenti rischiosi perché difficilmente trasferibili o vendibili. Per esempio, software o sistemi operativi possono essere sviluppati specificatamente per funzionare solamente con determinati dispositivi mentre investimenti tangibili – come macchinari o terre – possono, in teoria, essere facilmente vendibili a terzi.

Gli intangibili sono predisposti a promuovere sinergie – o complementarità – tra loro e nei diversi comparti produttivi, massimizzandone l'efficienza e il potenziale valore industriale. Se si pensa all'ultimo smartphone immesso nel mercato, il valore intrinseco del prodotto-merce è il risultato della sinergia tra il prodotto finale e diversi asset intangibili – come il software che fa funzionare il cellulare, il suo design che lo caratterizza e il brand con cui è pubblicizzato.

Gli intangibili subiscono inoltre un effetto *spillover*, vale a dire che i benefici prodotti da capitale intangibile tendono ad essere facilmente replicabili e imitabili da aziende concorrenti, incrementando il rischio di perdere profittabilità dal proprio investimento. Quando il primo iphone fu immesso nei mercati nel giugno del 2007, il suo design rivoluzionario a tutto schermo è stato velocemente adottato dai concorrenti, divenendo uno standard di mercato.

Se le risorse intangibili hanno difatti diverse proprietà di mercato, significa che non rappresentano un semplice cambiamento nelle preferenze dei flussi di investimenti ma che una loro crescente influenza nell'economia globale potrebbe avere degli impatti strutturali sulle dinamiche delle forze produttive.

Da una parte, come notato da Michael Roberts, l'accumulazione di capitale intangibile non porterebbe a un cambiamento della natura del capitalismo in un paradigma d'analisi marxista in quanto il concetto di "capitale" si riferisce al suo senso fisico e non in quanto conduttore di determinati rapporti di produzione e di relazioni sociali[7]. Allo stesso modo, Guglielmo Carchedi ha sottolineato che nell'economia della conoscenza vige la stessa logica di sfruttamento del capitale lavoro che caratterizza il capitalismo contemporaneo[8].

[7] Michael Roberts, "Capitalism Without Capital – Or Capital Without Capitalism?", in *Michael Roberts Blog*, 10 dicembre 2017, https://wp.me/pLequ-3Mu.

[8] Guglielmo Carchedi, "Old Wine, New Bottles and the Internet", in *Work Organisation, Labour & Globalisation*, vol. 8, n. 1 (Summer 2014), p. 69-87.

D'altra parte, nonostante queste critiche, è innegabile che l'emergere di un'economia intangibile abbia dei profondi effetti sull'organizzazione dell'economia globale che devono essere approfonditi per contestualizzare le sfide politiche, economiche e sociali che le società dovranno affrontare.

7.2 Intangibili e mercati

L'interazione tra le quattro proprietà degli intangibili – sinergie, *spillover*, costi sommersi e scalabilità – rischia di amplificare il pericolo di mercati altamente concentrati, in cui "un vincitore conquista quasi tutto (se non tutto) il piatto"[9]. La scalabilità di prodotti e servizi permette di espandere il proprio brand e i propri processi produttivi su scala globale senza costi aggiuntivi, creando una barriera di ingresso a nuovi concorrenti e facilitando l'emergere di grandi multinazionali dall'intenso sfruttamento di capitale intangibile. Inoltre, se effettivamente si crea valore dalla sinergia tra diversi asset intangibili e tangibili, una multinazionale sarà incentivata a massimizzare il proprio profitto sviluppando ecosistemi[10] in grado di offrire ai consumatori più prodotti e servizi. Qualora esista la percezione che i propri investimenti non garantiscono redditività per via dell'effetto *spillover*, molte aziende non saranno neppure incentivate ad investire in innovazione a meno di non avere una tale copertura di capitale finanziario da potersi permettere di immettere nel mercato prodotti e servizi a bassa profittabilità[11].

Questo dibattito sugli effetti degli intangibili nell'organizzazione economica si inserisce nella più ampia discussione sugli attuali trend macroeconomici, in particolare sulle cause che possono spiegare la concentrazione dei mercati globali e il differenziale produttivo tra le multinazionali leader e i concorrenti.

---

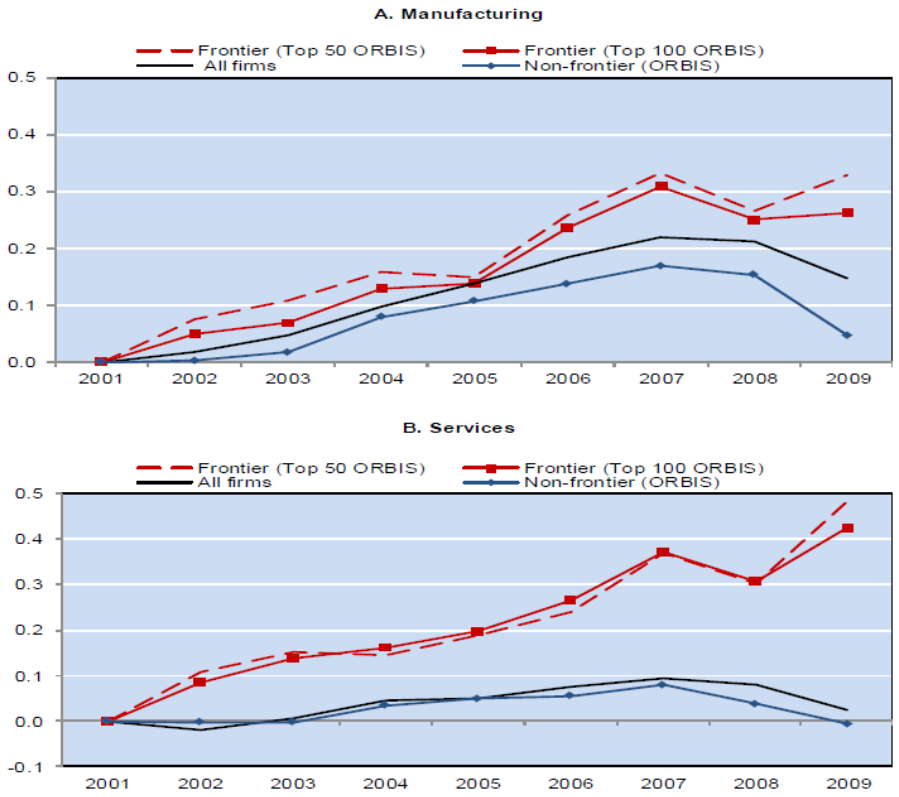
[9] Varun Ghotgalkar et al., "How the Digital Economy Is Changing Corporate Pricing and Inflation", in *AXA IM Research*, 22 agosto 2017, https://www.axa-im.com/documents/20195/859236/How+the+digital+economy+is+changing+corporate+pricing+and+inflation+20170822+en/0e395a9f-7e76-7468-c807-9a968b3abefb.

[10] Un ecosistema è un network di attività e organizzazioni interdipendenti che cooperano tra loro per massimizzare la capacità di operare nel mercato.

[11] Nicolas Crouzet e Janice Eberly, "Understanding Weak Capital Investment: the Role of Market Concentration and Intangibles", in *NBER Working Papers*, n. 25869, agosto 2018, p. 13-15.

Se gli effetti delle quattro proprietà principali degli intangibili fossero effettivamente quelli sopra descritti, l'economia globale dovrebbe mostrare dei mercati in cui un ristretto numero di multinazionali ha alti livelli di produttività rispetto ai concorrenti grazie all'inteso sfruttamento di intangibili. Coerentemente, da un recente studio dell'Organizzazione per la cooperazione e lo sviluppo economico (Ocse) è emerso come le prime cinquanta e cento aziende "*frontier*", cioè quelle con gli indici di produttività più alti, abbiano incrementato negli ultimi anni il differenziale di produttività rispetto alla concorrenza[12].

Figura 9 – Differenziale di produttività tra le imprese frontier e le concorrenti



Fonte: Dan Andrews, Chiara Criscuolo e Peter N. Gal, "Frontier Firms, Technology Diffusion and Public Policy", cit., p. 12.

[12] Dan Andrews, Chiara Criscuolo e Peter N. Gal, "Frontier Firms, Technology Diffusion and Public Policy: Micro Evidence from OECD Countries", in *OECD Productivity Working Papers*, n. 2/2015, https://doi.org/10.1787/5jrql2q2jj7b-en.

David Autor e altri hanno analizzato la concentrazione in diversi settori industriali negli Stati Uniti collegandola alla diminuzione dal fattore della forza-lavoro come componente nella creazione del valore. Le multinazionali leader tendono a implementare una filiera produttiva più tecnologica che aumenta l'efficienza, riducendo al contempo il bisogno di forza-lavoro, e che permette loro di conquistare quote di mercato grazie ad una maggiore produttività[13]. Negli ultimi vent'anni il 75 per cento delle industrie nordamericane ha subito dei processi di concentrazione a causa della maggiore profittabilità e capacità tecnologica delle aziende leader[14]. Già negli anni '90, John Sutton aveva previsto che un'evoluzione dei mercati verso prodotti ad alto valore di capitale intangibile avrebbe prodotto una distorsione in cui pochi attori avrebbero controllato il mercato immettendo servizi e prodotti dal basso margine costo-prezzo, e creando barriere per nuovi concorrenti[15].

In un recente lavoro Federico Díez e Romain Duval hanno analizzato il rapporto tra prezzo e costo dei prodotti per circa un milione di aziende nel mondo. Tra il 2000 e il 2015 tale rapporto è cresciuto in media del 6 per cento. Il 10 per cento delle imprese, quelle in cima alla classifica per costo/prezzo, sono risultate essere le più produttive, le più profittevoli e a più alta intensità di capitale intangibile. I due economisti del Fondo monetario internazionale (Fmi) ritengono che gli effetti di rete, lo sfruttamento di risorse intangibili e l'economia di scala siano divenuti i vantaggi comparati delle aziende leader che sono in grado di produrre barriere d'ingresso ai concorrenti[16]. Non stupisce quindi che le 575 imprese più redditizie generino tra il 20-22 per cento dei profitti corporate globali[17].

---

[13] David Autor et al., "The Fall of the Labor Share and the Rise of Superstar Firms", in *NBER Working Papers*, No. 23396 (maggio 2017), https://www.nber.org/papers/w23396.

[14] Gustavo Grullon, Yelena Larkin e Roni Michaely, "Are US Industries Becoming More Concentrated?", in *Review of Finance*, vol. 23, n. 4 (luglio 2019), p. 697-743, https://doi.org/10.1093/rof/rfz007.

[15] John Sutton, *Sunk Costs and Market Structure. Price Competition, Advertising, and the Evolution of Concentration*, Cambridge, MIT Press, 1991.

[16] Federico Díez e Romain Duval, "How to Keep Corporate Power in Check", in *IMF Blog*, 3 aprile 2019, https://blogs.imf.org/2019/04/03/how-to-keep-corporate-power-in-check.

[17] James Manyika et al., "'Superstars': The Dynamics of Firms, Sectors, and Cities Leading the Global Economy", in *McKinsey Global Institute Discussion Papers*, ottobre 2018, http://bit.ly/2ScrC5g.

In un eccellente studio, Mordecai Kurz ha calcolato che le imprese tecnologicamente più avanzate hanno un *surplus wealth*, cioè la differenza tra ricchezza prodotta (equity e debito) e il suo capitale, che in molti casi supera l'80 per cento della ricchezza prodotta[18]. I valori di *surplus wealth* più elevati sono riscontrati proprio nei settori più trasformati dall'It.

Tabella 2 – Le venti imprese americane con il più ampio *surplus wealth* nel 2015

20 Firms with Largest Surplus Values			20 Firms with Surplus Values Around the Mean			20 Firms with Smallest Surplus Values		
Firm Name	χ Value	Surplus Wealth	Firm Name	χ Value	Surplus Wealth	Firm Name	χ Value	Surplus Wealth
APPLE INC	1	435861	LIBERTY VENTURES	0	3552	YAHOO INC	1	-7283
ALPHABET INC	1	396179	FRONTIER COMMUN.	1	3539	WILLIAMS PARTNERS LP	0	-7496
AMAZON COM INC	1	294519	BLUE BUFFALO PET PRODU	0	3536	ENTERGY CORP	0	-7558
AT&T INC	1	269517	BLACKBAUD INC	1	3517	ICAHN ENTERPRISES LP	0	-7670
FACEBOOK INC	1	267902	FMC TECHNOLOGIES INC	0	3490	AES CORP	0	-7670
VERIZON COMM.	1	260112	TREEHOUSE FOODS INC	0	3480	PLAINS GP HOLDINGS LP	0	-9648
MICROSOFT CORP	1	258150	WILLIAMS COS INC	0	3462	ENERGY TRANSFER EQUITY	0	-10672
JOHNSON & JOHNSON	1	238127	OUTFRONT MEDIA INC	0	3431	NEWMONT MINING	0	-10759
PROCTER & GAMBLE CO	0.5	209646	AMERICAN WATER WORKS	0	3423	LEUCADIA NATIONAL	0	-12449
PFIZER INC	1	203586	PRA HEALTH SCIENCES INC	1	3406	ENERGY TRANSFER PARTN.	0	-13729
COMCAST CORP	1	177803	BRINKER INTL INC	0	3404	HESS CORP	0	-14465
GENERAL ELECTRIC CO	1	170531	BIO-TECHNE CORP	1	3401	FREEPORT-MCMORAN INC	0	-15417
COCA-COLA CO	0	167927	ACADIA PHARMACEUTICAL	1	3380	AGNC INVESTMENT CORP	0	-15787
ORACLE CORP	1	162979	CHARLES RIVER LABS INTL	1	3377	MARATHON OIL CORP	0	-17822
WAL-MART STORES INC	0	160896	CAVIUM INC	1	3370	STARWOOD PROPERTY	0	-19919
ALLERGAN PLC	1	160859	COMMUNICATIONS SAL& LS	0	3356	ANNALY CAPITAL MANAG.	0	-20543
PHILIP MORRIS	0	151843	WEX INC	1	3354	EXELON CORP	0	-21681
PEPSICO INC	0	149538	EPAM SYSTEMS INC	1	3342	FORD MOTOR CO	0	-27908
DISNEY (WALT) CO	1	147021	SONOCO PRODUCTS CO	0	3331	GENERAL MOTORS CO	0	-29675
IBM	1	135571	B&G FOODS INC	0	3327	CHEVRON CORP	0	-44148
Mean χ Value	0.78			0.45			0.05	

Nota: Valori in milioni di dollari 2015, dati senza disponibilità liquide estere.
Fonte: Mordecai Kurz, "On the Formation of Capital and Wealth…", cit., p. 12.

Seppure gli intangibili siano divenuti un fattore produttivo fondamentale in ogni industria, integrandosi e interagendo con risorse tangibili, essi rappresentano l'architettura essenziale dell'economia digitale nella quale si possono osservare delle dinamiche di competitività che accentuano il rischio di avere mercati altamente concentrati. I mercati digitali stanno massimizzando l'implementazione di modelli di business basati su due risorse intangibili: dati (*data-driven asset*) e hub.

Secondo Marco Iansiti e Karim Lakhani sono tre le dinamiche di mercato che caratterizzano l'economia digitale. La legge di Moore predice che la potenza di elaborazione dei computer si raddoppia ogni due anni. Ciò, combinato alla sempre più crescente inter-connessione tra le tecnologie digitali, permette di trasmettere e condividere informazioni ad un costo marginale bassissimo. La legge di Metcalfe, invece, suggerisce che il valore di una rete cresce in base al numero di nodi e utenti che interagiscono con

[18] Mordecai Kurz, "On the Formation of Capital and Wealth: IT, Monopoly Power and Rising Inequality", in *SIEPR Working Papers*, No. 17-016 (25 giugno 2017), https://siepr.stanford.edu/node/7278.

esso, i cosiddetti effetti di rete[19]. Per finire, il principio di Albert-László Barabási spiega che se il numero di transizioni di una rete cresce, il suo potere economico aumenta e si espande connettendo più consumatori, aziende e industrie. Quando un hub raggiunge un'economia di scala in un settore economico, avrà dei vantaggi comparati ad espandersi in altre industrie[20].

L'interazione tra queste tre dinamiche potrebbe produrre un "effetto domino" in cui si incentiverebbero catene del valore disintermediate in cui nuovi attori utilizzando le tecnologie digitali divengono dei medium indispensabili nell'interazione e nelle transizioni tra diversi gruppi economici (come per esempio tra consumatori finali e aziende). Alphabet, per esempio, ha ampliato i confini del suo core business da motore di ricerca generico a strumento di comparazione prezzi (Google Shopping), mappe (Google Maps), aggregatori di contenuti (Google News, YouTube, Google Books, Google Pay), negozio e-commerce (Google Pay), sistemi operativi (Android) o provider di sistemi di connessione nel settore automobilistico. Ma si può anche pensare a Uber che, dopo aver lanciato UberPop e UberX – servizi di noleggio con conducente (Ncc) e taxi –, ha introdotto nuovi servizi come UberEats, per la consegna a domicilio, o UberCargo.

Per renderla ancora più semplice. Sono esempi di disintermediazione la nuova funzione di Instagram che permette attraverso hyperlink di accedere ai negozi e-commerce che vendono i capi indossati nelle foto pubblicate sul social media; oppure l'applicazione Google Maps che segnala e suggerisce agli utenti ristoranti, bar o negozi nella zona in cui si stanno dirigendo.

In questa nuova logica di intermediazione l'aggregazione di dati diviene un fattore competitivo. La possibilità di accumulare e analizzare virtualmente dati su ogni aspetto delle attività sociali, economiche e politiche dei consumatori permette di incrementare radicalmente la conoscenza dei consumatori e di offrire loro prodotti e servizi *ad hoc*. Ciò potrebbe però produrre delle serie problematiche relative all'asimmetria informativa che si crea tra chi ha gli strumenti per accumulare e gestire

[19] Si ha un'esternalità di rete quando il beneficio che un individuo trae dall'utilizzo di un bene cresce al crescere del numero di utilizzatori di quel bene.

[20] Marco Iansiti e Karim Lakhani, "Managing Our Hub Economy", in *Harvard Business Review*, vol. 95, n. 5, (settembre-ottobre 2017), p. 84-92, https://hbr.org/2017/09/managing-our-hub-economy.

questi dati e chi no. Il pericolo, anche in questo caso, è che la superiore capacità informativa sui consumatori possa divenire una barriera d'entrata nei mercati e possa consolidare la creazione di rendite. Douglas Rushkoff ha coniato il paradigma di "capitalismo estrattivo" per spiegare il modello di business delle grandi società tecnologiche basato sulla continua ricerca volta ad accumulare e monetizzare più dati possibili per continuare a essere profittevoli in diversi settori[21].

7.3 Competitività e mercati

Gli effetti dell'economia degli intangibili sui mercati divengono fenomeni interessanti in quanto la competizione è nelle maggiori teorie economiche lo strumento per garantire una più efficiente allocazione delle risorse: la spinta essenziale per promuovere innovazione e produttività[22]. Il dibattito su un'eccessiva concentrazione del mercato digitale in mano a un numero ristretto di giganti del web è particolarmente vivo in relazione agli effetti negativi che potrebbe avere sull'innovazione e sulla concorrenza. Normalmente il mercato è caratterizzato da rendimenti decrescenti che stimolano la competitività. Gli asset digitali invece tendono a mostrare rendimenti crescenti facilitando il consolidamento nel mercato dell'attore con più dati a disposizione, la rete più consolidata o la più ampia scalabilità[23].

Nella letteratura economica esistono due visioni differenti sulla natura e sugli effetti del monopolio nel funzionamento del mercato.

Da una parte, Schumpeter parlava della distruzione creativa intrinseca al capitalismo come del moto dinamico dell'innovazione. Secondo la sua visione sarebbe l'innovazione stessa a creare le condizioni per posizioni di monopolio perché solo le imprese leader avrebbero i capitali per finanziare la ricerca e lo sviluppo di innovazione sulle quali poi cercano di produrre rendite il più a lungo possibile. Ma questo equilibrio statico verrebbe interrotto dalla capacità di un'altra azienda che con un prodotto

[21] Douglas Rushkoff, *Piovono pietre sui bus di Google. Come la crescita è diventata nemica della prosperità*, Viterbo, Stampa Alternativa/Banda Aperta, 2018.

[22] Raghuram G. Rajan e Luigi Zingales, "The Influence of the Financial Revolution on the Nature of Firms", in *NBER Working Papers*, n. 8177 (marzo 2001), https://www.nber.org/papers/w8177.

[23] Marco Iansiti e Karim Lakhani, "Managing Our Hub Economy", cit.

o un servizio innovativo rivoluziona il mercato creandosi una posizione monopolista e relative rendite[24]. Questo è anche l'approccio della Scuola di Chicago per la quale le situazioni di monopolio, quando esistenti, sarebbero solo temporanee perché l'aspettativa di generare tali rendite spinge le aziende concorrenti ad innovare a beneficio dei consumatori[25].

Applicando questa visione all'economia digitale, Tyler Cowen ritiene che i giganti tecnologici abbiano stimolato innovazione e che, anzi, con l'acquisto dei propri concorrenti abbiano massimizzato successivamente il loro potenziale innovativo[26]. Anche Hal Varian, capo economista di Google, ha ribadito che la competizione tra i giganti tecnologici nel mercato digitale si gioca nei diversi segmenti industriali più che all'interno di essi, e a livello globale più che nazionale. La continua evoluzione dell'innovazione beneficerebbe la competizione perché permette agli attori più piccoli di avere accesso a tecnologie che ne diminuiscono i fattori produttivi[27].

Al contrario, già dagli anni '80, Partha Dasgupta e Stiglitz ricordano che nei mercati non esiste solamente la concorrenza sul prezzo o sul prodotto ma anche quella determinata dall'innovazione[28]. Uno studio sulla competizione digitale, prodotto per il governo britannico da un gruppo di esperti, evidenzia come i processi di concentrazione siano intrinseci ai mercati digitali a causa degli effetti di rete[29]. Nel lungo termine si potrebbero dunque creare i presupposti per una distorsione del funzionamento dei mercati che comporterebbe prezzi più alti, meno innovazione e meno scelta per i consumatori. Il rapporto sostiene che il paradigma classico del diritto anti-trust è antiquato e non più in grado di inquadrare efficacemente gli sviluppi dell'economia digitale[30].

---

[24] Joseph A. Schumpeter, *Capitalismo, socialismo, democrazia*, Milano, Edizioni di Comunità, 1955.

[25] Arnold C. Harberger, "Monopoly and Resource Allocation", in Saul Estrin e Alan Marin (a cura di), *Essential Readings in Economics*, London, Macmillan, 1995, p. 77-90.

[26] Tyler Cowen, "Breaking Up Big Tech Would Be A Big Mistake", in *The Globe and Mail*, 17 aprile 2019, https://www.theglobeandmail.com/opinion/article-breaking-up-big-tech-would-be-a-big-mistake.

[27] Hal Varian, "No Hope of a Quiet Life in the Age of Disruption", in *The Financial Times*, 3 ottobre 2016, https://www.ft.com/content/ad4188dc-872d-11e6-a75a-0c4dce033ade.

[28] Partha Dasgupta e Joseph Stiglitz, "Uncertainty, Industrial Structure, and the Speed of R&D", in *The Bell Journal of Economics*, vol. 11, n. 1 (Spring 1980), p. 1-28.

[29] Digital Competition Expert Panel, *Unlocking Digital Competition*, London, HM Treasury, marzo 2019, https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel.

[30] Ibid., p. 6.

Seguendo la teoria sulle piattaforme digitali di Jean-Charles Rochet e Jean Tirole, nei mercati digitali i giganti del web possono sussidiare alcune attività all'interno del proprio ecosistema per offrire prodotti e servizi a un prezzo marginale pari a zero[31]. Alain Strowel e Wouter Vergote hanno sottolineato che, per esempio, il tradizionale test Ssnip[32] non è in grado di valutare effettivamente potenziali comportamenti anti-competitivi nel mercato digitale perché, in questo caso, non si ha come obiettivo l'innalzamento dei prezzi, bensì quello della conquista del consumatore con il relativo accesso e l'accumulazione dei dati personali degli utenti stessi[33].

Se effettivamente il valore commerciale dei dati e dei network delle piattaforme sono fattori produttivi, e quindi competitivi, si potrebbero realizzare i presupposti per un'asimmetria informativa distorta, naturale o creata dai mercati, che possono creare nuove barriere di ingresso.

7.4 Intangibili e le implicazioni socio-politiche

Le rivoluzioni tecnologiche determinano la trasformazione delle strutture produttive e creano nuovi rapporti di forza nell'economia: dalle compagnie commerciali in età coloniale alle grandi aziende petrolifere, dalle banche fino ai giganti tecnologici. In un recente saggio, l'economista Luigi Zingales ha ripreso un paradigma caro all'economia strutturalista per cui il potere economico si riflette sul potere politico. Con un parallelismo con la dinastia della famiglia Medici, che nel XV secolo utilizzò il proprio capitale monetario per ottenere potere politico finanziando il papato, Zingales sottolinea che le imprese tendono per propria natura a cercare di influenzare le istituzioni pubbliche per ottenere dei vantaggi economici[34]. Per contestualizzare cosa si intende per "potere" bisogna prendere

[31] Jean-Charles Rochet e Jean Tirole, "Platform Competition in Two-Sided Markets", in *Journal of the European Economic Association*, Vol. 1, n. 4 (giugno 2003), p. 990-1029, https://www.rchss.sinica.edu.tw/cibs/pdf/RochetTirole3.pdf.

[32] Small but significant non-transitory increase in price (Ssnip) è uno strumento economico utilizzato per valutare se i potenziali effetti sul welfare dei consumatori in caso di un incremento di un determinato servizio/prodotto offerto da un monopolista.

[33] Alain Strowel e Wouter Vergote, "Digital Platforms: To Regulate or Not to Regulate? Message to Regulators: Get the Economics Right First, then Focus on the Right Regulation", in Bram Devolder (a cura di), *The Platform Economy. Unravelling the Legal Status of Online Intermediaries*, Cambridge, Intersentia, 2019, p. 3-30.

[34] Luigi Zingales, "Towards a Political Theory of the Firm", in *The Journal of Economic*

in considerazione il lavoro di Steven Lukes che descrive le dimensioni del potere sia in termini di creazione e controllo dell'ambiente in cui vengono prese le decisioni, sia di esercizio del rispetto delle regole esistenti[35].

La discussione accademica sul presunto condizionamento esercitato dai poteri economici sulle istituzioni rappresentative e viceversa è ricca dal momento che le scelte politiche nazionali e sovranazionali regolamentano il funzionamento dei mercati. Gli stati-nazione e le imprese private sono quindi interdipendenti. I primi necessitano delle seconde per creare occupazione e finanziare le casse pubbliche attraverso la tassazione. Le seconde invece demandano ai primi l'imposizione dei diritti di proprietà privata e di sicurezza dei loro mezzi di produzione.

Di particolare interesse è poi l'approccio teorico di Susan Strange, elaborato già negli anni '70, che cerca di interpretare l'interazione tra politica e potere economico alla luce dell'emersione di grandi conglomerati privati. Paragonando due unità di misura forse troppo diverse tra loro, cioè il gettito fiscale di uno stato e i ricavi delle grandi multinazionali, alcuni studiosi hanno elaborato una classifica in cui queste ultime occuperebbero 71 posizioni nelle prime cento, rendendo la loro forza economica paragonabile, se non superiore, a quelli di molti stati[36].

Questo rapporto andrebbe valutato in termini di un potere strutturale – inteso come il potere "di influenzare l'agenda delle discussioni o di deciderla"[37] delineato da quattro dimensioni portanti – sicurezza, produzione, finanze e conoscenza – le quali, in competizione tra loro, cercano di ottenere vantaggi economici influenzando il potere politico. L'attuale crescita dell'importanza del ruolo della creazione, legittimazione, diffusione e sfruttamento delle risorse intangibili nell'economia globale potrebbe quindi cambiare i rapporti di forza tra queste quattro dimensioni in favore dell'industria della conoscenza[38].

Perspectives, vol. 31, n. 3 (Summer 2017), p. 113-130, https://www.jstor.org/stable/44321282.

[35] Steven Lukes, *Il potere. Una visione radicale*, Milano, Vita e pensiero, 2007.

[36] Milan Babic, Jan Fichtner e Eelke M. Heemskerk, "States versus Corporations: Rethinking the Power of Business in International Politics", in *The International Spectator*, vol. 52, n. 4 (novembre 2017), p. 20-43, https://doi.org/10.1080/03932729.2017.1389151.

[37] Susan Strange, *States and Markets*, 2. ed., London, Pinter, 1994, p. 25.

[38] Blayne Haggart, "New Economic Models, New Forms of State: The Emergence of the 'Info-Imperium' State", in Hanns Ullrich, Peter Drahos e Gustavo Ghidini (a cura di), *Kritika: Essays on Intellectual Property*, Cheltenham/Northampton, Edward Elgar, 2018, p. 159-188.

Con un semplice esercizio di osservazione, si nota che nel 2018 le prime cinque multinazionali per valore nel mercato azionario erano Apple, Google, Microsoft, Amazon e Facebook. Solo dieci anni prima la classifica era ben diversa: i primi cinque posti erano occupati da Exxon, General Electric, Microsoft, AT&T e Procter & Gamble. La forza finanziaria dei giganti tecnologici è anche testimoniata dalle 617 acquisizione fatte fino al 2016 per un valore aggregato superiore ai 128,5 miliardi di dollari[39].

Questa influenza è resa evidente soprattutto dalla loro crescente funzione strutturale nell'economia globale. Questi attori, infatti, controllano e gestiscono le infrastrutture e le tecnologie di intermediazione nelle quali le reti digitali si sviluppano. Come ha scritto Jeremy Ghez, "l'influenza dei Gafa (e non solo) deriva dalla loro abilità di ridefinire una serie di realtà politiche e sociali che sono il cuore dell'attuale comunità globale"[40].

Google, oltre a gestire il 91 per cento delle ricerche online con il suo motore di ricerca, ha il suo sistema operativo Android installato sul 79,8 per cento degli smartphone del mondo. Sommando tale percentuale al numero degli smartphone supportati da Ios, Apple e Google forniscono il sistema operativo al 97,26 per cento del mercato mondiale della telefonia mobile. Amazon ha registrato il 90 per cento delle vendite online in cinque categorie di prodotti e 310 milioni di clienti attivi. Facebook può contare su 2 miliardi di utenti registrati sul social media, 1 miliardo sull'app di messaggistica istantanea WhatsApp, 1,5 miliardi sul social media Instagram e su YouTube più di 1,8 miliardi di visite al mese.

Anche il mercato dei servizi tecnologici sta incentivando sempre più i giganti tecnologici ad integrarsi con i più disparati settori industriali che compongono l'economia. Per esempio, nel settore dei servizi di *cloud-computing*, Amazon Web Services, Microsoft Azure e Google Cloud, secondo alcune stime, gestirebbero più del 65 per cento del mercato. Un esempio ancora più chiaro è riscontrabile nella ricerca e sviluppo delle automobili senza conducente. I giganti tecnologici stanno sviluppando partnership (ad esempio il progetto e-Palette di Toyota e Amazon) e investendo (il finanziamento diretto di Amazon nella startup Aurora) in questo settore.

[39] Nicola Bilotta e Simone Romano, "Tech Giants in Banking: The Implications of a New Market Power", in *IAI Papers*, n. 19|13 (giugno 2019), p. 15, https://www.iai.it/en/node/10483.

[40] Jeremy Ghez, "Why U.S. Tech Giants Might Not Dominate The World After All", in *Forbes*, 16 novembre 2016, https://www.forbes.com/sites/hecparis/2016/11/16/why-us-tech-giants-might-not-dominate-the-world-after-all.

Delle 52 aziende che hanno ottenuto il permesso di fare test su questo tipo di autovetture, oltre a una decina di aziende automobilistiche classiche e numerose start-up specializzate, sono presenti sei giganti tecnologici tra cui Apple, Alphabet (Waymo), Baidu e Samsung Electronics[41].

Se la de-territorializzazione prodotta dalla digitalizzazione e le trasformazioni tecnologiche favoriscono le imprese più produttive in ogni industria, l'emersione di *superstart* con livelli di produttività e redditività superiori rispetto agli altri sarà sempre più probabile. Stiglitz ha giustamente sottolineato che questi processi d'accentramento del potere di mercato non hanno solamente conseguenze economiche ma anche sociali[42].

Con il suo lavoro pioneristico nel 2003 il premio Nobel Dale Mortensen teorizzò che il differenziale produttivo tra aziende potrebbe causare una dispersione del salario, incrementando di conseguenza la disuguaglianza di reddito. Secondo un recente studio, il divario tra le imprese che pagano i salari più alti e quelle con i salari più bassi nel medesimo settore industriale è cresciuto del 12,3 per cento dal 2001 al 2012[43]. Questa divergenza è particolarmente accentuata nelle industrie in cui è aumentato lo spread di produttività. La differenza di produttività spiegherebbe circa metà del divario tra i salari delle diverse aziende nel medesimo settore industriale. Anche la ricerca di Autor conferma come nei segmenti industriali in cui la trasformazione It ha avuto un più forte impatto, la dispersione dei salari sia cresciuta[44].

A fronte di questo effetto regressivo della concentrazione dei mercati sul reddito da lavoro bisogna anche considerare che la progressiva importanza assunta dagli intangibili potrebbe mitigare l'effetto redistributivo della tassazione. Secondo uno studio dell'Ocse, in tutta l'area Ocse e G20 circa il 10 per cento del profitto aggregato dell'imposta sul reddito delle società viene erosa attraverso pratiche di *profit-shifting*, il cui valore è stato stimato essere di circa 240 miliardi di dollari nel 2014 e di 2,1 trilioni di dollari nel periodo 2005-2014.

---

[41] State of California Department of Motor Vehicles: *Permit Holders (Testing with a Driver)*, https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/permit.

[42] Joseph Stiglitz, "Inequality, Stagnation, and Market Power", cit.

[43] Giuseppe Berlingieri, Patrick Blanchenay e Chiara Criscuolo, "The Great Divergence(s)", in *OECD Science, Technology and Industry Policy Papers*, n. 39 (maggio 2017), p. 20, https://doi.org/10.1787/953f3853-en.

[44] Walter Frick, "Understanding the Debate Over Inequality, Skills, and the Rise of the 1%", in *Harvard Business Review*, 21 dicembre 2015, https://hbr.org/2015/12/understanding-the-debate-over-inequality-skills-and-the-rise-of-the-1.

Le risorse intangibili riescono a sfuggire più facilmente all'attuale sistema di tassazione – basato su due criteri antiquati come la residenza (che impone imposte sulla produzione) e l'origine, che invece è composta principalmente sull'imposta sul valore aggiunto (Iva). Così facendo si divide il potere fiscale tra il Paese in cui un'impresa risiede e quello in cui opera. Grazie allo sviluppo delle tecnologie e degli intangibili nelle catene di creazione del valore, oggi è facile generare profitti in diverse nazioni senza avere una presenza fisica in loco, riuscendo quindi a pagare le imposte in nazioni a fiscalità agevolata.

Secondo alcune stime, quindici aziende *superstart* statunitensi avrebbero da sole più di 776 miliardi di dollari in Paesi considerati paradisi fiscali. Per esempio, Apple avrebbe 111,3 miliardi offshore, Microsoft 76,4 miliardi di dollari e Google 38,9 miliardi di dollari.

La digitalizzazione dell'economia richiederebbe investimenti sociali e reti di sostegno ai "perdenti" dei cambiamenti tecnologici. A tal fine, gli stati-nazione dovranno riuscire a imporre un'equa tassazione a coloro che, sfruttando gli intangibili, stanno conquistando i mercati globali. In caso contrario sarà difficile immaginare un'efficace compensazione alle fratture sociali che si stanno progressivamente creando[45].

Conclusioni

Il mondo sta rapidamente cambiando. L'economia globale sembra dipendere sempre di più da risorse intangibili che ne trasformano le strategie e le politiche industriali. Questo cambiamento strutturale dei modi di produzione ha dei profondi effetti anche sulle dinamiche di competizione nei mercati.

Gli asset intangibili tendono ad avere delle proprietà di mercato che facilitano l'emergere di un numero limitato di imprese molto produttive e profittevoli, incrementando il gap tra aziende leader e inseguitrici. Gli asset intangibili di valore sono solitamente scalabili. A fronte di un cospicuo investimento iniziale, tali servizi e prodotti possono essere replicati infinite volte con costi aggiuntivi minimi o inesistenti. Tali aziende traggono inoltre vantaggi economici dallo sviluppo di sinergie tra differenti risorse

[45] Ocse, *Addressing the Tax Challenges of the Digitalisation of the Economy*, 12 febbraio 2019, https://www.oecd.org/tax/beps/public-consultation-document-addressing-the-tax-challenges-of-the-digitalisation-of-the-economy.pdf.

intangibili e non, appropriandosi quindi facilmente dei benefici prodotti da risorse intangibili di altre aziende. La globalizzazione del digitale massimizza queste tendenze.

La concentrazione dei mercati non ha solamente implicazioni economiche ma anche politiche. Questi enormi attori privati potrebbero avere un potere politico indiretto paragonabile a quello di uno stato-nazione. L'interpretazione semplicistica che considera un'azienda come una serie di contratti[46], scevra e distaccata dalla realtà politica in cui è regolata, non inquadra adeguatamente gli equilibri di potere esistenti nella società.

L'ascesa dell'economia degli intangibili potrebbe aver anche mutato i rapporti di forza in favore dell'industria della conoscenza a scapito della finanza e della produzione[47]. I giganti tecnologici sono divenuti rapidamente le imprese a più alta capitalizzazione e redditività nei mercati azionari. La loro influenza non risiede semplicemente nel potere finanziario ma, soprattutto, nell'essere gli attori che gestiscono le infrastrutture e i nodi sui quali è costruita l'architettura digitale.

Queste trasformazioni richiedono un ripensamento delle politiche pubbliche per cercare di massimizzarne il potenziale positivo dell'innovazione. I governi dovrebbero, a tal fine, riporre particolare attenzione ai "perdenti" della digitalizzazione, penalizzati da una crescente disuguaglianza di reddito causata in parte dal differenziale produttivo tra le imprese leader e le altre. In quest'ottica, per garantire sia parità di condizioni tra aziende sia la mitigazione degli effetti negativi redistributivi, i governi dovrebbero cercare di cooperare a livello multilaterale per sviluppare un sistema di tassazione equa della ricchezza prodotta dagli intangibili.

Le rivoluzioni tecnologiche non sono malvagie o benigne/positive o negative *a priori*. Dunque, il destino dei cambiamenti strutturali dei modi di produzione dipende primariamente dal modo in cui gli stati-nazione affrontano le sfide alle quali sono esposti.

[46] Michael C. Jensen e William H. Meckling, "Theory of the Firm: Managerial Behaviour, Agency Costs and Ownership Structure", in *Journal of Financial Economics*, vol. 3, n. 4 (ottobre 1976), p. 305-360, https://doi.org/10.1016/0304-405X(76)90026-X.

[47] Blayne Haggart, "New Economic Models, New Forms of State", cit.

8.
Algor-etica: il dibattito internazionale sull'identità morale degli algoritmi informatici

Alessandro Picchiarelli

Fin dalla sua comparsa sulla Terra, l'uomo si è dovuto confrontare con tutta una serie di limiti che il suo corpo e la sua natura gli imponevano. In confronto agli altri esseri viventi, infatti, esso appariva almeno all'inizio della sua storia quasi come un essere insignificante, preda dei grandi animali e bisognoso di adattarsi all'ambiente che trovava intorno a sé. Tuttavia con il passare dei secoli esso ha sviluppato tutta una serie di capacità che lo hanno reso superiore a tutti gli altri esseri viventi: ha imparato ad esprimersi attraverso il linguaggio potenziando le sue abilità cognitive, si è organizzato in tribù, ha iniziato a coltivare il terreno, ha maturato raffinate tecniche di caccia. La cosa che però gli ha permesso di far fronte a molti dei suoi bisogni è stata la creazione di artefatti tecnologici che ovviassero ai suoi limiti. Essi rappresentano il modo attraverso il quale l'uomo comprende sé stesso e l'ambiente che lo circonda e sono qualunque tipo di strumento inventato dall'uomo e attraverso cui egli plasma l'ambiente circostante lasciandosi a sua volta plasmare da esso.

In questi ultimi decenni lo sviluppo tecnologico e informatico ha prodotto tutta una serie di artefatti tecnologici che hanno portato l'uomo ad interagire in maniera nuova con il suo corpo, con gli altri esseri umani e con l'ambiente in cui esso vive. Tra questi artefatti bisogna sicuramente considerare gli algoritmi informatici. Infatti,

> nelle nostre società, i calcoli hanno un posto ben più centrale di quanto non immagini chi vorrebbe ridurli a funzioni matematiche

> e respingere la tecnica al di fuori della società, quasi si trattasse di un *alien* minaccioso. I calcolatori fabbricano la nostra realtà, la organizzano e la orientano. Producono convenzioni e sistemi di equivalenza che selezionano certe cose a discapito di altre, impongono una gerarchizzazione di valori che va progressivamente disegnando i quadri cognitivi e culturali delle nostre società[1].

Tutto questo avviene ogni giorno nella nostra vita, anche se non ne siamo pienamente consapevoli, e determina dei cambiamenti sociali di non poco valore. Sono molteplici gli ambiti nei quali gli algoritmi informatici hanno oramai un ruolo importante. Nella pubblica sicurezza i sistemi di polizia predittiva sono una realtà assodata. Esistono tantissimi sistemi che, sulla base dell'analisi ambientale e dei fattori di rischio legati a un quartiere o a una zona cittadina, cercano di prevedere dove accadranno crimini e chi ha una maggiore probabilità di commetterli. In ambito militare esiste un settore di studio e di sviluppo di armi intelligenti che cercano di sostituirsi all'uomo soprattutto nelle missioni e nelle situazioni più pericolose. In ambito medico i sistemi di assistenza e di precisione negli interventi chirurgici sono ampiamente utilizzati e si stanno sviluppando tecniche di acquisizione e di elaborazione di immagini sempre più sofisticate per la selezione degli embrioni nelle tecniche di riproduzione assistita o per prevenire malattie serie come il cancro o per gestire il trapianto di organi. Per non parlare di tutti i sistemi intelligenti di assistenza per le persone (malate, sole o anziane) o dei veicoli a guida autonoma che si stanno diffondendo in molte città. Questi sistemi di intelligenza artificiale hanno la capacità di imparare progressivamente dalla loro esperienza per migliorare sempre di più le proprie prestazioni. Anche la vita personale, gli interessi e i sentimenti umani non sono un ambito che viene escluso dagli algoritmi informatici. Ci sono moltissime applicazioni, dette *dating app*, che promettono di aiutare ad incontrare una persona che, attraverso la profilazione e la statistica, ha un'alta probabilità di poter essere la propria anima gemella. Oppure si parla sempre di più di arte algoritmica o di creatività computazionale per descrivere quelle opere d'arte che non sono il frutto del genio artistico dell'uomo ma che vengono prodotte per mezzo di sistemi di Ia e di algoritmi informatici.

Tutto ciò rende evidente il fatto che

[1] Dominique Cardon, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei big data*, Milano, Mondadori, 2016, p. 7.

> assistiamo al sorgere di nuove sfide: la sfida di cominciare a concepire l'uomo come animale informazionale al fianco di altri, all'interno dell'infosfera; la sfida di farsi carico di una nuova società, la società dell'informazione, cresciuta molto più rapidamente della capacità dell'uomo di sviluppare solide radici concettuali, etiche e culturali in grado di comprenderla, gestirla e orientarla verso il bene comune e lo sviluppo[2].

Questa nuova fase della storia dell'uomo, nella quale i dati e l'informazione hanno un ruolo centrale, ha determinato la nascita di un nuovo ambito di riflessione morale, da molti definito algor-etica, nel quale si cerca di capire che ruolo abbiano gli algoritmi informatici nelle valutazioni morali che l'uomo è chiamato a compiere. Tali riflessioni risultano essere particolarmente cogenti non solo perché appare evidente la necessità di progettare algoritmi che rispettino determinati principi etici e che non siano "disumanizzanti", ma anche perché la loro sempre maggiore autonomia, imprevedibilità e capacità di influenzare la comprensione che l'uomo ha di sé stesso e del mondo, rende necessaria una riflessione sullo statuto morale da associare a questi artefatti tecnologici.

È proprio per questo motivo che da alcuni decenni si è iniziato a riflettere sulla possibilità di associare le categorie tipiche del discorso morale riguardanti l'uomo anche ad altri tipi di entità compresi gli algoritmi informatici. Alla base di tutto ciò c'è la constatazione che sia gli agenti umani che quelli non umani sono caratterizzati da un certo impatto nel mondo (dall'apprendimento, dall'empatia e da una finalità) e questo ha portato a parlare di agenti morali artificiali (Ama). L'introduzione di questa nuova forma di agentività ha innescato un dibattito molto forte soprattutto in ambito europeo e americano e ha generato una separazione tra coloro che sostengono che un agente artificiale è anche un agente morale, coloro che rifiutano questa posizione e parlano di entità morali invece che di agenti morali e coloro che si pongono in una posizione intermedia rispetto a quasi moralità legata alla definizione di un nuovo soggetto in cui la cooperazione tra l'uomo e l'algoritmo diventa l'elemento fondante per parlare della moralità degli artefatti. In questo capitolo ci si concentrerà su queste tre posizioni tralasciando la posizione di chi ritiene che gli artefatti siano semplicemente strumenti creati dell'uomo e che quindi

[2] Paolo Benanti, *Le macchine sapienti. Intelligenze artificiali e decisioni umane*, Bologna, Marietti 1820, 2018, p. 95.

non abbiano nessuna rilevanza morale e quella di chi associa la rilevanza morale dell'artefatto tecnologico alla sua funzione che determinerebbe anche il valore morale dell'artefatto stesso. Queste riflessioni saranno utili per caratterizzare il discorso sull'algor-etica che verrà affrontato nel quarto paragrafo.

8.1 Gli algoritmi come agenti morali

I sostenitori dell'agentività morale degli artefatti tecnologici partono dalla costatazione che è necessario riflettere sullo statuto morale di tutte quelle realtà che oggi influenzano le decisioni umane. Già Hans Jonas nel 1979 aveva avanzato l'ipotesi che in un futuro non troppo lontano sarebbe stato necessario estendere il dominio delle considerazioni morali per tener conto dell'esistenza di quegli oggetti inanimati e non biologici che non potevano essere trascurati nell'analisi morale[3]. A partire da queste considerazioni, Luciano Floridi, docente italiano di Filosofia e di Etica dell'informazione all'Università di Oxford, ha sviluppato un sistema nel quale dimostra che l'agentività morale degli artefatti tecnologici è qualcosa di possibile. Egli parte dalla constatazione che tutto ciò che compone l'universo, esseri viventi e non, singoli individui e strutture sociali più complesse, va considerato come un oggetto informazionale, che lui chiama *inforg*, all'interno di un sistema complesso definito infosfera:

> non siamo immobili al centro dell'universo (la rivoluzione copernicana), non siamo innaturalmente separati e diversi dal resto del regno animale (la rivoluzione darwiniana), e siamo molto lontani dall'essere menti isolate interamente trasparenti a se stesse […] (la rivoluzione freudiana). […] Sotto molti profili non siamo entità isolate quanto piuttosto organismi informazionali interconnessi, o inforg, che condividono con agenti biologici e artefatti ingegnerizzati un ambiente globale costituito in ultima analisi dalle informazioni, l'infosfera[4].

[3] Hans Jonas, *Il principio responsabilità. Un'etica per la civiltà tecnologica*, Torino, Einaudi, 1990.

[4] Luciano Floridi, *La rivoluzione dell'informazione*, Torino, Codice, 2012, p. 10-11. Si veda anche Luciano Floridi e J.W. Sanders, "Artificial Evil and the Foundation of Computer Ethics", in *Ethics and Information Technology*, vol. 3, n. 1 (marzo 2001), p. 55-66.

Proprio perché tutti gli *inforg* sono caratterizzati da un livello almeno minimo di informazione, essi vanno sempre rispettati come destinatari di un'azione morale anche se non tutti gli *inforg* possono essere considerati anche agenti morali. Inoltre essi non hanno tutti lo stesso contenuto informativo per cui alcuni richiederanno un rispetto e un riconoscimento morale maggiore rispetto agli altri. Floridi arriva alla conclusione che ad un certo livello di astrazione anche gli oggetti artificiali possono essere considerati agenti morali come gli esseri umani. Infatti, affinché un *inforg* possa essere considerato un agente è necessario che goda di tre proprietà che il filosofo individua nell'interattività, ossia nella capacità di interagire con l'ambiente circostante, nell'autonomia, ossia la possibilità di cambiare il proprio stato interno indipendentemente dalle interazioni con l'ambiente esterno, e nell'adattabilità, ossia nella capacità di imparare dall'esperienza e di cambiare così le proprie regole di transizione da uno stato ad un altro. Queste tre proprietà possono valere anche per un algoritmo informatico quando viene considerato al giusto livello di astrazione per cui esso può essere sicuramente considerato un agente. Inoltre, all'interno di questo sistema etico, un elemento fondamentale è rappresentato dall'entropia ossia dalla misura di ogni tipo di distruzione, alterazione o corruzione di un oggetto informazionale: più l'informazione viene danneggiata o perduta e più l'infosfera si impoverisce e l'entropia aumenta. Un agente sarà detto morale se è in grado di realizzare azioni che possono far aumentare o diminuire il livello di entropia dell'infosfera. Per cui un'azione sarà moralmente buona se diminuisce il livello di entropia generale del sistema e sarà non buona se invece aumenta l'entropia totale dell'infosfera. Da evidenziare è il fatto che queste azioni non richiedono il possesso di particolari stati mentali come ad esempio il dubbio o la certezza, di intenzioni o di volontà in quanto rappresentano un processo informativo rivolto verso un certo destinatario. Secondo Floridi, quindi, quello che è necessario fare è spostare l'analisi morale dall'approccio classico antropocentrico e orientato all'azione compiuta da un certo agente individuale ad un approccio ontocentrico e orientato al destinatario dell'azione che viene posta in essere per valutare se l'entropia complessiva dell'infosfera viene accresciuta o diminuita dall'azione considerata. In questo modo è possibile separare la responsabilità morale, che richiede intenzione, consapevolezza e libertà, dall'imputabilità morale che non richiede queste prerogative tipicamente umane. Quello che Floridi afferma è che ad un certo livello di astrazione ogni agente, umano o non, presenta un fine che orienta il suo comportamento indipendentemente dalla libertà, dall'in-

tenzione o dalla consapevolezza di realizzarlo in quanto questo determina soltanto che l'imputabilità morale diventi anche responsabilità morale piena[5].

John Sullins, docente della Sonoma State University in California, si pone su una linea molto simile. Egli afferma che la pervasività che caratterizza gli artefatti tecnologici e la velocità con cui essi progrediscono non devono essere trascurate nelle valutazioni etiche perché in un futuro molto prossimo l'uomo sarà in grado di interagire con essi come fa con gli altri esseri viventi[6]. Per tale motivo è necessario definire i presupposti etici che fondano questa nuova relazione tra l'uomo e gli artefatti in modo da stabilire quale statuto morale può essere associato ad essi. Sullins rifiuta il fatto che gli artefatti tecnologici possano essere considerati solo come semplici strumenti di mediazione e afferma la possibilità di poterli considerare come agenti morali senza stati mentali. Anche lui parte dalla teoria dei livelli di astrazione e si concentra su tre aspetti ritenuti fondamentali per definire lo statuto morale degli artefatti: l'autonomia, l'intenzionalità e la responsabilità. L'autonomia viene riferita all'idea che l'artefatto possa agire senza essere sotto il diretto controllo di un qualunque altro agente o utente. Se questo avviene (e si pensi ad alcuni sistemi di intelligenza artificiale che oggi si sostituiscono ai processi decisionali umani o ai sistemi di *machine learning* in cui l'apprendimento determina decisioni che non sono prevedibili), l'artefatto presenta una sua agentività indipendente da colui che lo ha realizzato e pensato e può causare danni o portare miglioramenti nel contesto in cui opera in maniera del tutto imprevedibile. L'intenzionalità viene considerata come la capacità di voler agire per ottenere un certo risultato e di volerlo fare in un certo modo. In questo senso la dimensione morale dell'intenzionalità negli artefatti tecnologici appare come la predisposizione a raggiungere gli obiettivi preposti senza provocare danni al contesto in cui l'artefatto opera. Infine, la responsabilità appare come la possibilità di imputare all'artefatto le conseguenze delle sue azioni e delle sue decisioni. Sullins riconosce che ad oggi non è possibile parlare di un'agentività morale piena per gli artefatti ma che è comunque

[5] Luciano Floridi, *The Ethics of Information*, Oxford, Oxford University Press, 2013. Si veda anche Luciano Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, Giappichelli, 2009.

[6] John P. Sullins, "When Is a Robot a Moral Agent", in *International Review of Information Ethics*, n. 6 (dicembre 2006), p. 23-30, http://www.i-r-i-e.net/inhalt/006/006_Sullins.pdf.

possibile, ad un certo livello di astrazione, parlare di un artefatto come di un agente morale anche se non perfettamente uguale ad un agente morale umano. In questo senso, egli apre il campo alle considerazioni sulla quasi moralità che verranno introdotto a seguire.

Michael Anderson, dell'Università di Hartford, e Susan Leigh Anderson, dell'Università del Connecticut, affermano che è possibile creare un agente artificiale morale che sia autonomo, interattivo, intenzionale e a cui poter almeno imputare le conseguenze delle sue azioni e propongono una serie di passi da fare per realizzare tutto ciò. Questi passaggi prevedono la rappresentazione e la determinazione dei principi etici alla base del funzionamento dell'artefatto, l'incorporazione di questi principi nell'algoritmo che determina il funzionamento del sistema, la possibilità che l'algoritmo possa agire anche senza una piena conoscenza di tutte le variabili in gioco e la scelta, tra le varie possibilità di azione realizzabili dal sistema, di quella azione che ottimizza i risultati attesi e che permette di raggiungere i fini stabiliti[7].

8.2 Gli algoritmi come entità morali

Il principio su cui si basano i sostenitori della non agentività degli algoritmi informatici è molto semplice. Un algoritmo, benché possieda una certa rilevanza morale legata al fatto di influenzare notevolmente le scelte umane, non può mai essere considerato un sistema indipendente e autonomo ma va sempre posto in relazione agli esseri umani che lo hanno sviluppato o che lo utilizzano e al contesto sociale e culturale nel quale esso viene sviluppato.

Secondo Deborah Johnson, dell'Università della Virginia, un'azione per essere qualificata come morale deve presentare almeno cinque caratteristiche essenziali[8]. Innanzitutto deve essere realizzata da un agente caratte-

[7] Michael Anderson e Susan Leigh Anderson, "Machine Ethics: Creating an Ethical Intelligent Agent", in *AI Magazine*, vol. 28, n. 4 (Winter 2007), p. 15-26, https://doi.org/10.1609/aimag.v28i4.2065.

[8] Deborah G. Johnson, "Computer Systems: Moral Entities But Not Moral Agents", in *Ethics and Information Technology*, vol. 8, n. 4 (novembre 2006), p. 195-204, https://nissenbaum.tech.cornell.edu/papers/computer_systems.pdf. Si veda anche Deborah G. Johnson e Merel Noorman, "Artefactual Agency and Artefactual Moral Agency", in Peter Kroes e Peter-Paul Verbeek (a cura di), *The Moral Status of Technical Artefacts*, Dordrecht, Springer, 2014, p. 143-158.

rizzato da desideri, credenze, stati mentali e dall'intenzione di voler agire. Questo determina un evento in cui l'agente stesso fa qualcosa muovendo anche il suo corpo per realizzarlo. Questo evento è conseguenza dello stato interno dell'agente e determina un cambiamento di esso e dell'ambiente circostante. Infine, l'effetto di tale azione è sempre rivolto verso un destinatario che può essere danneggiato o aiutato. La Johnson osserva che anche nel caso di un sistema informatico in cui agisce un algoritmo è possibile distinguere tra eventi esterni e interni al sistema per cui la seconda e la terza condizione non creano problemi di distinzione tra un agente umano e uno artificiale. Analogamente, indipendentemente dal tipo di agente, ogni azione determina un cambiamento di stato interno ed esterno ed è rivolta verso un destinatario per cui neanche la quarta e la quinta caratteristica costituiscono un problema. Quella che mostra una qualche criticità è la prima condizione. Infatti un agente morale artificiale, secondo i sostenitori della non agentività morale, non possiede nessuna volontà o intenzione di agire e inoltre non esiste quella libertà di poter agire o di non farlo che è un presupposto fondamentale di ogni valutazione morale. Anche nel caso degli algoritmi di *machine learning*, in cui l'apprendimento determina il comportamento del sistema facendo pensare ad una certa indeterminatezza nella modalità in cui il sistema agirà, il modo in cui il sistema apprende è legato alla comprensione del programmatore che lo ha sviluppato. L'intenzionalità di un agente artificiale, sostiene Johnson, è quindi sempre legata alla sua funzionalità e non si può parlare di un agente morale ma soltanto di un'entità morale che entra a far parte del processo di decisione morale, la quale rimane prerogativa esclusiva dell'essere umano. Johnson fa infine riferimento al concetto di autonomia, la quale presenta, secondo l'autrice, due importanti connotazioni. La prima riguarda la capacità di poter scegliere liberamente di agire e di farlo in un certo modo mentre la seconda riguarda la possibilità di agire indipendentemente da qualcuno. Soltanto nel primo caso si può parlare di una dimensione morale dell'azione ma questa connotazione di autonomia non riguarda gli artefatti tecnologici che possono al massimo presentare soltanto il secondo tipo di autonomia. La decisione morale, e quindi la responsabilità morale per la decisione presa, rimane perciò prerogativa umana pur riconoscendo il fatto che essa può essere vista come la combinazione del comportamento umano e dell'influenza su tale comportamento che l'entità artificiale coinvolta nel processo di decisione determina.

Su una posizione simile si pone anche Vincent Wiegel, della HAN University of Applied Sciences in Olanda. Egli afferma che un agente artifi-

ciale potrebbe agire come se avesse credenze e potrebbe anche apparire simile nel comportamento a un essere umano ma questo non autorizza ad associare ad esso uno statuto morale analogo a quello umano poiché soltanto l'uomo è in grado di associare un significato alle azioni che compie. Per questo motivo, come concludeva la Johnson, l'agentività morale degli agenti artificiali non può mai essere valutata separatamente da quella dell'uomo[9]. Infatti, qualunque siano i presupposti filosofici adottati, secondo Wiegel un algoritmo informatico avrà sempre un impatto morale ma non potrà mai essere pensato come un agente morale. Analogamente Peter-Paul Verbeek, un filosofo olandese dell'Università di Twente, afferma che oggi l'agentività morale va considerata come un fenomeno ibrido che coinvolge sia l'uomo che gli artefatti tecnologici. Tuttavia l'uomo e gli artefatti tecnologici appartengono a due mondi diversi: l'uomo è caratterizzato dall'intenzionalità e dalla libertà mentre gli artefatti sono entità strumentali[10]. Quello che è urgente, allora, è capire come questa mutua relazione tra uomo e tecnologia influenzi l'intenzionalità e la libertà umana: è necessario riconcettualizzare il fenomeno morale alla luce della nuova realtà tecnologica nella quale l'uomo vive ed opera. Infatti, la mediazione che gli artefatti tecnologici operano non solo costituisce un aiuto per l'uomo nello svolgere le sue attività, ma anche un modo nuovo di fare esperienza e di percepire l'ambiente che lo circonda. Per questo motivo se escludere dal discorso morale gli artefatti risulta essere riduttivo, è necessario tuttavia mantenere la giusta distinzione tra il concetto di agente umano, che è prettamente legato all'uomo, e di entità morale, che può essere associato agli artefatti. Rispetto agli altri filosofi che sostengono la non agentività morale degli artefatti tecnologici, Verbeek rilegge quindi l'intenzionalità e la libertà alla luce del ruolo di mediazione assunto dagli artefatti. Egli afferma che se si intende l'intenzionalità nel senso latino del termine, ossia nel senso del dare una direzione, è facile concludere che anche gli artefatti hanno una certa forma di intenzionalità in quanto orientano le decisioni che l'uomo può prendere e questo avviene, nel caso degli algoritmi informatici, non solo secondo quanto i programmatori o gli utilizzatori determinano

[9] Vincent Wiegel, "The Ethics of IT-Artefacts", in Luciano Floridi (a cura di), *The Cambridge Handbook of Information and Computer Ethics*, Cambridge, Cambridge University Press, 2010, p. 201-218.

[10] Peter-Paul Verbeek, "Some Misunderstandings About the Moral Significance of Technology", in Peter Kroes e Peter-Paul Verbeek (a cura di), *The Moral Status of Technical Artefacts*, Dordrecht, Springer, 2014, p. 75-88.

ma anche secondo il modo in cui un sistema apprende (si pensi ai sistemi di apprendimento automatico). Analogamente, rileggendo la libertà come la capacità di agire in un certo modo, si può associare una certa forma di libertà anche agli artefatti tecnologici. Alla luce di tali riflessioni, la sua conclusione è che, pur non essendo possibile parlare allo stesso modo di agentività per l'uomo e per gli artefatti, è comunque possibile affermare che esiste una mutua collaborazione tra queste due realtà e che entrambe, secondo le loro caratteristiche e specificità, rientrano nel discorso morale.

8.3 La quasi moralità degli algoritmi informatici

La terza linea di pensiero è forse quella più recente e anche quella ancora meno dibattuta. Il principio alla base di questo approccio è che allo stato attuale dello sviluppo tecnologico non è ancora possibile assegnare una piena agentività morale agli artefatti tecnologici come quella che si riconosce agli esseri umani ma è comunque necessario tener conto della grande analogia, non uguaglianza, esistente tra gli agenti morali umani e gli agenti morali artificiali.

Il primo contributo preso in esame proviene ed è stato sviluppato da Philip Brey, filosofo americano docente all'Università di Twente, che afferma che non è possibile non tener conto delle differenze tra un agente morale umano e un artefatto tecnologico. Per questo motivo propone un'etica che lui definisce strutturale che non assegna agli artefatti un'agentività morale ma solo un ruolo morale e che si pone come un'etica complementare a quella classica[11]. In particolare, le entità artificiali che hanno un impatto morale nella realtà sono definite fattori morali in quanto determinano direttamente il risultato di un'azione e agiscono sia a livello sociale, influenzando i valori che le società percepiscono e agendo sulle strutture o reti costituite sia da esseri umani che da entità non umane, e sia a livello personale, determinando modi diversi di azione e possibilità nuove di scelta. Tuttavia non tutti i fattori morali sono anche agenti morali. Infatti per esserlo essi devono possedere la capacità di prendere decisioni morali, devono essere in grado di non agire in modo immorale e devono poter essere considerati responsabili per le loro azioni. Brey

[11] Philip Brey, "From Moral Agents to Moral Factors: The Structural Ethics Approach", in Peter Kroes e Peter-Paul Verbeek (a cura di), *The Moral Status of Technical Artefacts*, Dordrecht, Springer, 2014, p. 125-142.

conclude che molti sistemi di intelligenza artificiale, benché ancora non presentino una piena capacità di prendere decisioni morali e non siano perfettamente in grado di evitare di agire immoralmente, stanno progredendo così velocemente che non è possibile escludere che in un futuro prossimo queste due condizioni possano essere soddisfatte. Quello che rimane problematico è associare la responsabilità morale a un agente artificiale in quanto, non possedendo una libera volontà, non ha la capacità di provare piacere o dolore rispetto a una punizione che gli può essere inflitta. Per questo motivo egli parla di "agenti quasi-morali" per indicare il fatto che essi sono simili, ma non uguali, agli agenti morali umani e preferisce parlare di imputabilità e non di responsabilità per questi agenti.

A delle conclusioni simili giungono anche Christian Illies, dell'Università di Bamberg in Germania, e Anthonie Meijers, dell'Università di Eindhoven in Olanda. Essi affermano che esistono due tipi di responsabilità: quella di chi volontariamente, consapevolmente e liberamente compie un'azione e quella di chi influenza il modo di agire di qualcun altro. Nel primo caso si può parlare di responsabilità di primo grado mentre nel secondo caso di responsabilità di secondo grado. Quest'ultima non diminuisce la responsabilità di primo grado di un soggetto, ma rende responsabile l'entità che ha influenzato le scelte del soggetto agente, avendo modificato le possibilità di scelta a disposizione del soggetto principale. Per cui un artefatto tecnologico può possedere un certo tipo di responsabilità che, pur non essendo ancora piena e di primo grado, è sicuramente una responsabilità di secondo grado[12].

8.4 L'etica degli algoritmi informatici

L'introduzione delle tre diverse linee di pensiero riguardo la moralità degli artefatti tecnologici permette ora di potersi concentrare sul fatto che, indipendentemente dalla posizione che si assume, è necessaria una riflessione sulle implicazioni morali che la presenza degli artefatti determinano nella vita dell'uomo. In modo particolare tra gli artefatti tecnologici che oggi influenzano di più l'esistenza umana ci sono sicuramente di algoritmi informatici la cui presenza è tanto pervasiva quanto relativamente ignorata. Gli

[12] Christian F.R. Illies e Anthonie Meijers, "Artefacts, Agency, and Action Schemes", in Peter Kroes e Peter-Paul Verbeek (a cura di), *The Moral Status of Technical Artefacts*, Dordrecht, Springer, 2014, p. 159-184.

algoritmi informatici, infatti, arrivano a sostituirsi all'uomo in alcune decisioni e in alcuni ambiti tipicamente riservati agli esseri umani. Per questo motivo, all'interno del contesto dell'etica, si sta sempre di più espandendo un ambito di studio che molti definiscono algor-etica cioè etica degli algoritmi. L'algor-etica si basa sul presupposto che il filosofo italiano Cosimo Accoto ha ben tratteggiato ossia che "la soggettività deve essere ripensata e riconcettualizzata in quanto non più individuabile come prerogativa privilegiata di attori umani singoli"[13]. Questa considerazione apre il campo al fatto che non è più sufficiente considerare l'uomo nella sua individualità ma è necessario ripensarlo come soggetto che si trova a cooperare, anche nel suo agire morale, con altre soggettività non necessariamente umane come gli algoritmi informatici. Questo modello costituito dalla cooperazione tra l'uomo e l'artefatto secondo Paolo Benanti, teologo italiano e docente presso la Pontificia Università Gregoriana di Roma, potrebbe aiutare da un lato l'uomo ad acquisire familiarità con i criteri etici e funzionali che sono alla base degli algoritmi informatici e dall'altro lato a tradurre tutto ciò che è umano in categorie e linguaggi comprensibili dai sistemi informatici[14]. Dunque si comprende facilmente come la rivoluzione informatica stia riconfigurando lo statuto ontologico dell'intera realtà tanto da condurre diversi filosofi, tra cui Luciano Floridi, a concludere che

> Non vi è un termine per indicare questa nuova forma radicale di costruzione, cosicché possiamo usare il neologismo *riontologizzare* per fare riferimento al fatto che tale forma non si limita solamente a configurare, costruire o strutturare un sistema (come una società, un'auto o un artefatto) in modo nuovo, ma fondamentalmente comporta la trasformazione della sua natura intrinseca, vale a dire della sua ontologia. In tal senso le Ict non stanno soltanto ricostruendo il mondo: lo stanno *riontologizzando*[15].

E tutto questo comporta che l'esistenza non sia più legata al supporto fisico che la caratterizza ma al poter interagire e scambiare informazioni con le altre soggettività[16].

---

[13] Cosimo Accoto, *Il mondo dato. Cinque brevi lezioni di filosofia digitale*, Milano, Egea, 2017, p. 93.

[14] Paolo Benanti, *Le macchine sapienti*, cit., p. 113-114.

[15] Luciano Floridi, *La rivoluzione dell'informazione*, cit., p. 13.

[16] Paolo Benanti, *La condizione tecno-umana. Domande di senso nell'era della tecnologia*, Bologna, EDB, 2016.

La possibilità di poter interagire non è qualcosa di strumentale ma un aspetto fondamentale nel discorso morale. Per questo motivo Paolo Benanti individua alcune caratteristiche che gli artefatti tecnologici, e quindi gli algoritmi informatici, dovrebbero avere affinché questa cooperazione sia significativa. Queste caratteristiche sono molto simili a quelle che già sono state menzionate nei paragrafi precedenti. In particolare la cooperazione deve basarsi sulla capacità reciproca di poter capire le intenzioni dell'altro per poter anticipare cosa l'altro vuole e per poter essere in grado di agire di conseguenza. In questo senso la capacità di sapersi adattare è un requisito fondamentale che già molti sistemi di intelligenza artificiale e di *machine learning* iniziano a presentare anche in maniera robusta. L'adattabilità porta con sé un'altra proprietà ossia la capacità di saper valutare come ciascuna soggettività prende le sue decisioni: è il problema della cosiddetta trasparenza algoritmica che deve fare i conti con i diritti di copyright propri delle aziende sviluppatrici e con la riservatezza dei dati a cui i sistemi attingono. Il trattamento dei dati comporta anche il fatto che non si debbano escludere certi tipi di dati a favore di altri per garantire che la cooperazione sia il più oggettiva possibile: questo garantisce un'affidabilità che permette all'uomo di potersi fidare dell'artefatto e all'artefatto di potersi sviluppare e di apprendere nel modo più oggettivo possibile evitando pregiudizi che porterebbero a valutazioni e a decisioni non corrette. Infine essendo l'uomo non soltanto razionalità ma anche emotività, l'artefatto deve saper tener conto e interagire anche con questo aspetto umano sviluppando una certa forma di empatia che permetta di entrare in relazione con questa parte più intima e personale dell'essere umano[17].

Affinché si possa tentare di fondare il discorso morale relativo agli algoritmi informatici è però necessario riflettere sulle categorie fondamentali che lo descrivono e cioè la consapevolezza, la libertà, la responsabilità e l'intenzionalità. A tal proposito, va osservato che l'intelligenza propria degli algoritmi informatici è sempre un'intelligenza specifica e relativa all'ambito rispetto al quale questo artefatto si trova ad agire e per il quale è progettato. Per cui non è possibile per un algoritmo avere un tipo di consapevolezza generale come quella umana ma si dovrà sempre parlare di una forma di consapevolezza specifica e pratica. Similmente, non si può affermare l'esistenza di una libertà come quella umana quanto piuttosto di una capacità di poter agire in un certo modo. Tale capacità impatta anche la libertà dell'uomo che vede ampliato lo spettro di azio-

[17] Paolo Benanti, *Le macchine sapienti*, cit., p. 118-122.

ne e di decisione che normalmente gli appartiene e tutto questo avviene in una maniera che non è sempre prevedibile e che dipende dal modo in cui gli algoritmi imparano e cambiano il loro comportamento in base all'esperienza che hanno acquisito. In questo spazio di imprevedibilità (*accountability gap*) rientra il discorso sulla responsabilità. Si è già visto che si tende a distinguere tra responsabilità e imputabilità. Tuttavia anche questa distinzione non è così pacificamente accettata tanto che sono moltissime le definizioni che vengono recuperate per dibattere su questo tema. Si pensi ai concetti di responsabilità distribuita[18] o di responsabilità surrogata[19] o alla responsabilità di primo e secondo grado[20]. Questa categoria rimane comunque fondamentale nel dibattito sull'agentività morale degli algoritmi informatici in quanto coinvolge tutta una serie di soggetti che intervengono nella progettazione, nello sviluppo e nell'uso di questi artefatti e per questo motivo, ad oggi, è uno dei nodi centrali del discorso affrontato in questo capitolo. Altrettanto problematico è il dibattito sull'intenzionalità degli algoritmi informatici. Secondo Paolo Benanti, l'intenzionalità va intesa come la capacità "di poter aggiustare i [propri] fini guardando la persona e cercando di capire qual è l'obiettivo adeguato in quella situazione"[21]. Tutto questo è possibile secondo Carl Mitcham, filosofo della tecnologia dell'Università di Saas-Fee in Svizzera, perché è credibile rileggere le credenze, i desideri e le intenzioni proprie dell'uomo come elementi appartenenti anche agli algoritmi informatici. Infatti,

> le credenze, costituendo le informazioni di stato di un agente, sono memorizzate in un database. I desideri o obiettivi sono programmati nei dispositivi in modo tale che essi trasformino specifici input in specifici output. Le intenzioni poi selezionano da un repertorio di piani o sequenze di movimenti ciò che permette di ottenere la funzione input-output desiderata[22].

---

[18] Hannah Arendt, *Responsabilità e giudizio*, Torino, Enaudi, 2010; Karl Jaspers, *La questione della colpa. Sulla responsabilità politica della Germania*, Milano, Cortina, 1996.

[19] Deborah G. Johson e Thomas M. Powers, "Computers as Surrogate Agents", in Jeroen van den Hoven e John Weckert (a cura di), *Information Technology and Moral Philosophy*, Cambridge, Cambridge University Press, 2008, p. 251-269.

[20] Christian F.R. Illies e Anthonie Meijers, "Artefacts, Agency, and Action Schemes", cit.

[21] Paolo Benanti, "Il lavoro nell'epoca della Machina sapiens", in *Oikonomia*, a. 16, n. 3 (ottobre 2017), p. 13, https://www.oikonomia.it/images/pdf/2017/ottobre/03-Benanti.pdf.

[22] Carl Mitcham, "Agency in Humans and in Artifacts: A Contested Discourse", in Peter Kroes e Peter-Paul Verbeek (a cura di), *The Moral Status of Technical Artefacts*, Dordrecht, Springer, 2014, p. 14. Traduzione dell'autore.

Ovviamente queste considerazioni lasciano aperto il campo a critiche, espresse soprattutto da parte di coloro che non riconoscono possibile un'agentività morale per gli artefatti tecnologici pur accettando il fatto che anche per questa quarta categoria è necessario un discorso molto approfondito sul concetto di intenzione e di intenzionalità.

Conclusioni

La presenza degli artefatti tecnologici e degli algoritmi informatici nella vita quotidiana dell'uomo porta con sé alcune considerazioni che, alla luce dell'analisi svolta, diventano spunti di riflessione ulteriore. Innanzitutto è evidente la necessità di definire una governance che garantisca il rispetto della dignità umana pur riconoscendo e auspicando un sempre maggiore progresso tecnologico. Tutto ciò va fatto tenendo conto delle sollecitazioni che emergono a livello internazionale, rileggendo e proponendo nuove categorie che possano affiancarsi a quelle tradizionali o almeno cerchino di risolvere la tensione linguistica che viene generata dall'utilizzo di certi termini tipici del discorso morale classico nell'ambito degli artefatti. In questo contesto appare evidente l'urgenza di ovviare alle lacune che risultano presenti nel discorso sull'agentività morale sia a livello filosofico che a livello etico. Si tratta di esplicitare il senso profondo di alcune categorie per capire se veramente il loro significato possa essere esteso anche agli agenti artificiali oppure se sia necessario introdurre un'etica complementare a quella tradizionale. Se da un lato le maggiori aziende mondiali chiedono indicazioni etiche che possano orientare la programmazione e la produzione di algoritmi informatici, e più in generale di artefatti tecnologici, dall'altro lato diventa necessaria una seria riflessione interdisciplinare che porti ad un dialogo costruttivo tra le varie competenze. Un contributo prezioso può venire anche dalla teologia morale che, a partire dalla riaffermazione del principio del bene comune e dei principi di giustizia ed equità sociale, può aiutare a scoprire quali direttive etiche dovrebbero essere implementate negli algoritmi informatici. Infatti, attraverso la tecnica è possibile scoprire i valori e la moralità di una società per cui essa va sempre orientata verso il bene comune e lo sviluppo integrale dell'uomo[23]. Inoltre, essendo gli artefatti tecnologici

[23] Paolo Benanti, "Tecnologia e sviluppo umano nella Caritas in veritate", in *Il Regno - Documenti*, n. 1/2014, p. 55.

"una realtà multidimensionale che contiene al suo interno tanto un'intenzionalità, che inclina ad agire in un certo modo, quanto una costituzione culturale, che si fa mediatrice di valori"[24], non è possibile considerarli come meri strumenti senza una moralità, ma essi vanno sempre pensati come attività strutturate del vivere umano per cui possono diventare occasioni di bene e di autentico sviluppo integrale umano ma anche occasioni di disumanizzazione se non sono orientati alla promozione autentica dell'essere umano e del creato.

Un'altra considerazione riguarda il fatto che la riflessione sullo statuto morale degli artefatti tecnologici si concentra prevalentemente in Europa e negli Stati Uniti. Sono praticamente assenti contributi dagli altri continenti se non sporadici interventi dall'India dove ci si concentra principalmente sul concetto di agentività morale e sulla possibilità per l'intelligenza artificiale di replicare facoltà proprie della mente umana[25]. Tutto ciò pur risultando evidente che molti Paesi, come il Giappone, sono leader nello sviluppo tecnologico e nel progresso raggiunto nell'antropomorfizzazione dei robot e nell'evoluzione dell'intelligenza artificiale e degli algoritmi di *machine learning*. Sensibilizzare sulla necessità di riflettere a livello internazionale sulle implicazioni morali degli artefatti tecnologici può sicuramente aiutare anche a ovviare a problemi di più ampio raggio come il *digital divide* o il rischio di disumanizzazione dell'uomo.

Infine, pur essendo vero che ad oggi non è possibile mettere sullo stesso piano un agente morale artificiale e un agente morale umano, rimane evidente la velocità con cui gli artefatti tecnologici stanno evolvendo e nessuno può escludere categoricamente che in un futuro molto prossimo queste differenze saranno annullate o notevolmente ridotte. Questa velocità rende ancora più urgente una seria riflessione anche a fronte delle nuove conquiste nell'ambito della computazione quantistica e nella sempre maggior ottimizzazione degli algoritmi informatici. Quello che risulta essere evidente è che questo aumento di potere e di capacità produttive non è stato accompagnato da un adeguato sviluppo dell'essere umano circa la responsabilità che ne deriva e dalla comprensione dei valori che ad esso sono associati[26].

---

[24] Ibid., p. 59.

[25] Rajakishore Nath e Vineet Sahu, "The Problem of Machine Ethics in Artificial Intelligence", in *AI and Society*, 19 ottobre 2017. Il primo è dell'Università di Bombay mentre il secondo dell'Università del Kanpur.

[26] Francesco, Lettera enciclica *Laudato sì*, 24 maggio 2015, AAS 107, 2015, p. 105.

Di fronte a una realtà sempre nuova e in continua evoluzione, come quella degli algoritmi informatici, anche la comprensione della società, del mondo in cui l'uomo vive, della cultura e dell'uomo stesso vengono inevitabilmente ad essere influenzate. La natura relazionale dell'essere umano chiede di essere riletta alla luce di queste nuove conquiste per ribadire che, in un contesto globale sempre più digitalizzato e ricco di opportunità ma anche di rischi, la tecnica deve essere sempre un motivo di crescita per l'uomo che può, anche attraverso di essa, scoprire potenzialità, capacità e risorse che lo aiutino ad essere ogni giorno più autenticamente umano, senza smarrire quei valori e quei principi che la tecnica può aiutare a proteggere e a incentivare ma che può anche far smarrire in derive tecnocratiche e alienanti.

Finito di stampare nel mese di settembre 2019
con la tecnologia *print on demand*
presso il CentroStampa "*Nuova Cultura*"
p.le Aldo Moro n. 5, 00185 Rome
www.nuovacultura.it
per ordini: ordini@nuovacultura.it

[Int_9788833652467_17x24col_LM02]