Rapporto

IL 5G E IL "NUOVO" PARADIGMA DI SICUREZZA DELL'UNIONE EUROPEA. REGOLE A TUTELA DI AUTONOMIA TECNOLOGICA E SOVRANITÀ

Maurizio Mensi

Sintesi

La rete 5G, per la connettività pervasiva e l'automazione intelligente che induce, è destinata a costituire la piattaforma tecnologica portante della società e dell'economia del futuro. Tuttavia le sue vulnerabilità potrebbero essere sfruttate per compromettere infrastrutture critiche, sottrarre dati sensibili e personali, incidere sugli stessi processi democratici ormai sempre più basati sulle infrastrutture digitali. Benché l'approccio al riguardo sia diversificato da paese a paese, trattandosi di sicurezza nazionale, la risposta dell'UE assume le forme di un "nuovo" modello, integrato e olistico, basato su un quadro articolato di regole, secondo le competenze attribute dal Trattato UE. L'obiettivo è quello di proteggere dati, sistemi e reti secondo i più elevati parametri di sicurezza. In una dimensione globale in cui si scontrano Stati Uniti e Cina, l'autonomia tecnologica dell'UE diventa condizione per l'esercizio di una sovranità che consenta agli Stati membri di tutelare sicurezza e interesse nazionale fronteggiando il rischio di influenze estere e minacce cyber, in linea con la propria collocazione atlantica. Alla base, la consapevolezza che garantire integrità e sicurezza delle reti 5G comporta la verifica tecnica dell'intera "catena di fornitura" (*supply chain*) e l'adeguatezza dei vari contraenti anche sotto il profilo strategico e regolamentare. Il che significa rendere efficiente e competitivo il sistema produttivo, a beneficio di cittadini e imprese. In sostanza, con riferimento al 5G l'UE ha avviato un cantiere normativo che riqualifica la propria azione anche a livello strategico, basato su un assetto giuridico a geometria variabile ed un concerto istituzionale simile a quello a suo tempo previsto in tema di comunicazioni elettroniche. Si tratta di un strategia multilivello a cui sono chiamati a contribuire soggetti pubblici e privati, istituzioni e imprese, a cui l'UE offre una serie di strumenti condivisi che ogni Stato membro può utilizzare per fronteggiare le minacce e mitigare i rischi secondo un approccio armonizzato, a salvaguardia dello stesso mercato unico. In tal senso il ruolo di stimolo e guida che l'Unione europea sta esercitando sul piano normativo assume anche rilevanti riflessi geopolitici, in sintonia con la sua storia e a protezione dei suoi valori.

Indice

1. CYBERSPAZIO E REGOLE NEL CAPITALISMO DELLA SORVEGLIANZA

1.1 La Rete come *common global medium*

Come rileva Norberto Bobbio, "*L'unico modo di intendersi quando si parla di democrazia, in quanto contrapposta a tutte le forme di governo autocratico, è di considerarla caratterizzata da un insieme di regole, primarie o fondamentali, che stabiliscono chi è autorizzato a prendere le decisioni collettive e con quali procedure*".

Ma le regole sono espressione e forma di una determinata società, di cui disciplinano organizzazione e modalità d'azione; sono quindi legate a storia, specifiche tradizioni culturali, grado di sviluppo e condizioni socio-economiche.

Tale concezione è peraltro legata ad un mondo in cui i sistemi non comunicavano fra loro e l'interazione reciproca, fra uomini e istituzioni, era condizionata dai mezzi di comunicazione. Soltanto partire dagli anni '50, con il diffondersi della televisione, questi hanno incominciato a mostrare la loro straordinaria forza espansiva, abilitandoci al confronto delle idee, con uno sguardo rivolto al mondo e alle sue varie espressioni, mettendoci in condizione di verificare la veridicità delle notizie e l'autorevolezza delle fonti informative.

Internet ha il merito di aver portato a compimento tutto questo. Alla sua *disruptive innovation*, la rivoluzione tecnologica che ne è alla base, con i *Big Data* e l'*e-government*, la "neutralità" della Rete e la sua portata democratica, va il riconoscimento per aver accelerato il passaggio ad una società della conoscenza basata sull'interconnessione e sui dati, in cui la tecnologia dà voce a un numero sempre più ampio di soggetti ed il saperne fare uso diventa elemento fondamentale e "abilitante" (per usare un termine oggi alquanto abusato) per cittadini e imprese[1].

Common global medium, internet rappresenta infatti sempre più lo strumento e la modalità precipua attraverso cui l'individuo si pone in relazione con i suoi simili ed i pubblici poteri ed è messo in condizione di esercitare appieno i propri diritti di cittadinanza, diventando motore e veicolo di conoscenza, trasparenza e innovazione. Ecco perché, come rileva David Weinberger, filosofo statunitense, l'architettura della Rete riflette i vecchi sogni della democrazia: tutte le persone sono uguali, tutte le idee hanno le stesse opportunità e le barriere alla partecipazione civile sono abbassate.

Internet e le nuove tecnologie diventano quindi elementi chiave del nuovo assetto sociale ed economico mondiale, in cui il *network* diventa la forma dominante di organizzazione e la *Netpolitik* impone ormai tempi e modalità d' azione, ridefinisce il concetto di sovranità e di giurisdizione e la differenza fra l'essere connessi o meno delinea la linea di demarcazione fra società evolute ed arretrate. Si tratta di un nuovo ecosistema basato su piattaforme digitali che operano e su cui transitano ingenti quantità di dati, che favorisce l'*e-commerce* attraverso l'interscambio di tali

[1] Si veda *La Rete fra tecnologia e diritto,* M. MENSI, in "*Il diritto del Web*", M. Mensi - P. Falletta, Padova, 2018, p. 22.

dati, generando sviluppo e rendendo possibile ai governanti misurare l'efficacia delle misure da adottare in base al risultato degli altri, mediante il confronto con le migliori pratiche, in un processo di ridefinizione dello stesso principio di autorità e progressiva disintermediazione dei poteri costituiti.

Appurato che la Rete costituisce uno strumento essenziale per il funzionamento della democrazia, la prassi dimostra come essa sia efficace soprattutto laddove già sia presente un'arena democratica, in un contesto di regole e valori condivisi, un sostrato civile ed economico adeguato. Le stesse forme dell'attuale democrazia rappresentativa possono trarre dalla Rete e dal mutato scenario tecnologico, che diventa anche sociale e politico, una nuova linfa, tale da ridefinire procedure più efficaci, per il coinvolgimento dei cittadini non soltanto nel procedimento che ne precede l'adozione ma anche nel contenuto delle decisioni che li riguardano, per un più proficuo rapporto fra rappresentanti e rappresentati. In tal modo internet si qualifica come autentico *engine of change*, strumento di "democrazia continua" suscettibile di incidere e migliorare i processi politici e sociali.

Internet ha infatti decentralizzato i processi informativi, infrangendo l'aura d'inaccessibilità che ammantava le autorità pubbliche e la "globalizzazione comunicativa" ha accresciuto la trasparenza delle istituzioni, favorendo la collaborazione tra i diversi organismi politico-amministrativi ed il controllo sul potere, riducendo il ruolo di interdizione degli intermediari e incoraggiando forme alternative di partecipazione, come quella stimolata dai *Social Network* con il loro tipico "effetto domino".

In tal senso gli strumenti tecnologici hanno mostrato la capacità di operare una vera e propria rivoluzione.

Tuttavia le ombre che i recenti sviluppi evidenziano ci inducono anche a considerare i rischi e le ambiguità del mito di una democrazia senza intermediari, che può anche tradursi in ultima analisi nella dissoluzione e ridefinizione dello stesso concetto di cittadinanza. Possiamo infatti ormai convenire sul fatto che sia illusorio ritenere che la Rete costituisca di per sé lo strumento salvifico che consente la partecipazione diretta *tout court* del cittadino alle dinamiche sociali e politiche che lo riguardano e che automaticamente trasforma la democrazia rappresentativa. Ancora più degli altri mezzi di comunicazione di massa, date le sue caratteristiche peculiari, può infatti diventare strumento di controllo funzionale ad un nuovo "capitalismo della sorveglianza"[2] che talora diventa uno straordinario amplificatore per messaggi semplificati e tesi apodittiche che sono destinate a suscitare adesione acritica più che a stimolare dibattito, riflessione e partecipazione consapevole.

1.2. Libertà e regole, internet e democrazia

Se manca una disciplina condivisa delle modalità con cui si estrinsecano le manifestazioni dei cittadini sulla Rete e la loro declinazione all'interno dei processi deliberativi, il superamento dei meccanismi consolidati di democrazia rappresentativa (che pure può trovare in internet gli elementi e gli stimoli per una

[2] S. ZUBOFF, *The age of surveillance capitalism*, 2019.

proficua rigenerazione) si rivela illusorio e di difficile realizzazione. In proposito, Lawrence Lessig segnala che "*il cyberspazio, lasciato a se stesso, difficilmente potrà mantenere le promesse di libertà e di maggiore partecipazione dei cittadini alla vita pubblica. Potrebbe anzi divenire un perfetto strumento di controllo*"[3].

Non vi può essere libertà senza regole*,* nel mondo *online* come in quello *offline, e o*ccorre evitare di inseguire il facile mito di una democrazia senza intermediari che giunge a definitivo compimento grazie ad internet. Al riguardo devono soccorrere educazione, consapevolezza, regole e valori condivisi, per un'interazione immune da semplificazioni e distorsioni, con l'obiettivo di perseguire una effettiva "inclusione digitale". È a tali elementi che è affidato il compito di provvedere alla tutela del diritto di informare ed essere informati, garantendo altresì la sicurezza delle persone e degli Stati.

Soltanto in tal modo ci si assicura che la Rete non diventi strumento di diffusione e amplificazione delle disuguaglianze ma continui ad essere veicolo di libertà e trasparenza, affinché il potenziale creativo delle nuove tecnologie accresca le possibilità di confronto aperto fra idee, per una conoscenza libera e pluralista.

Il diritto normalmente segue, quasi mai precede, una rivoluzione come quella originata dalla *disruptive innovation* indotta dall'affermarsi del digitale. Di qui alcune domande: quali regole e procedimenti per il governo della Rete, quali sono i soggetti deputati a stabilirle e a farle rispettare, come conciliare l'universalità di internet con la sovranità declinante degli Stati nazionali, quali strumenti utilizzare per assicurare sicurezza ai dati su di essa veicolati. Ma ancora di più si pone, a monte, l'interrogativo di fondo che attiene al rapporto tra internet e democrazia, vale a dire la questione più delicata: gli sviluppi della Rete, l'internet delle cose e le applicazioni dell'intelligenza artificiale sono davvero destinati a rafforzare l'esercizio delle pratiche democratiche e a favorire il passaggio dalle tradizionali forme di democrazia rappresentativa a forme più evolute di una democrazia partecipativa operante dal basso? Oppure si rischia di verificarsi proprio l'effetto opposto a quello auspicato, vale a dire l'accelerazione della crisi già in atto delle istituzioni rappresentative, suscettibile di aprire la strada a modelli autoritari fondati sul controllo, sulla sorveglianza e sulla manipolazione dell'opinione pubblica[4]?

Internet – come noto - ha natura transnazionale e al contempo territoriale, quindi mette a dura prova l'applicazione delle regole ordinarie domestiche, non perché esse non siano valide, ma perché si trovano a confliggere con quelle di ciascuno

[3] L. LESSIG, *Introduction*, in *Free Software*, *Free Society*. *The Selected Essays of Richard M. Stallman*, Boston, 2002.

[4] Sul nuovo modello di ingegneria sociale che si sta sperimentando a Singapore e *"che potrebbe presto essere applicato altrove; un grande fratello che usa le nuove tecnologie per il controllo delle persone"* si veda D. DE KERCKHOVE, *Big data e algoritmi. Il governo delle macchine, lo spettro della «datacrazia»*, in Avvenire.it, 12 novembre 2016.

Stato. Non a caso, con il termine "*governance*"[5] si intende il coordinamento tra soggetti privati e pubblici coinvolti nella gestione della Rete, che si pone come un mezzo "anarchico per natura" in quanto transazionale, delocalizzato, perennemente in evoluzione, aperto all'accesso e pluralista. Internet viene dunque disciplinata tenendo conto di queste sue caratteristiche, in modo che non ne siano compromesse la libertà e la neutralità. La dimensione digitale ha messo altresì in discussione il modello che vede nello Stato il principale soggetto abilitato a porre le regole, poiché le attività dispiegate in Rete travalicano i confini nazionali, stimolando l'autoregolamentazione a livello internazionale e la riflessione sul problema dell'aterritorialità, per cui appare necessario individuare norme comuni a sistemi giuridici separati[6].

Ecco perché la regolazione di internet si pone come una sorta di banco di prova per il diritto, che si confronta con l'ineludibile necessità di adottare istituti adeguati alle peculiarità di un fenomeno ormai non più nuovo, ma dalla sconvolgente portata eversiva.

Certamente nella nostra società la richiesta di disciplinare le forme di innovazione è sempre molto presente e trasversale a diverse discipline ma, come spesso succede, soprattutto di fronte ad un fenomeno di notevole diffusione e dalle molteplici implicazioni, il diritto e la regolamentazione hanno il problema di come inquadrare tali manifestazioni entro gli schemi ed i parametri di riferimento.

In ogni caso è per lo più riconosciuto come la richiesta di nuove regole non sempre risponda a criteri di efficienza economica o giuridica e nella nostra società è presente un indirizzo "naturale" verso una sovra-regolamentazione in ogni aspetto della vita sociale e privata che talora rischia di diventare patologico.

Per riprendere una celebre frase di Luigi Einaudi, dobbiamo "*conoscere per deliberare*". Tuttavia, se si ritiene che la libertà individuale, l'evoluzione culturale e l'efficienza economica siano essenziali per il nostro sviluppo, allora occorre essere molto cauti al riguardo, tenendo presente che la regolazione rappresenta sempre un costo, come indica con chiarezza l'OCSE nei suoi vari Rapporti in tema di *Regulatory Reform,* sia per chi la elabora sia per i destinatari[7].

---

[5] Sul ruolo della *governance* nell'arena pubblica e gli strumenti attraverso i quali questa si esplica, si veda G. DI GASPARE, *Gli strumenti negoziali della governance esterna e della governance istituzionale,* in Amministrazione in Cammino, 2007.

[6] Sulle problematiche relative all'aterritorialità della Rete, si v., *ex multis*, sent. n. 16307/2011 della Corte di Cassazione sulla diffamazione sul web come reato di evento e non di condotta (residenza dell'imputato come foro speciale per la Rete); e i casi riuniti C-509/09 e C-161/2010 della Corte di giustizia dell'Unione europea circa la competenza del giudice del luogo in cui la vittima di una diffamazione via internet ha il suo centro di interessi o del giudice che si trova negli Stati in cui si è diffusa la notizia, dal momento che l'offesa può essere percepita anche in altri territori a causa dell'aterritorialità della Rete.

[7] Conviene al riguardo conviene tener presente la lezione della Corte europea dei diritti dell'uomo che, pur in assenza di norme specifiche relative alla Rete, ha svolto e continua svolge un ruolo essenziale, interpretando in modo evolutivo e lungimirante l'art. 10 della Convenzione del 1950, così da conferire tutela alla libertà di espressione *online*. In particolare la giurisprudenza della Corte è

Internet presenta, fra le varie caratteristiche, quella di dare voce a un numero sempre più ampio di soggetti[8], ed in tal senso costituisce uno straordinario motore e veicolo di conoscenza e innovazione, *lato sensu*[9]. La dottrina ha ampiamento indagato la relazione tra internet e democrazia nella società globalizzata attuale[10], rilevando come la sua diffusione abbia generato maggiore trasparenza e circolazione di informazioni in tutti gli ambiti della vita economica, politica e sociale, accelerando il processo di "democratizzazione reale" dell'*Information Society*[11] attraverso il decentramento dei centri decisionali che sono messi in comunicazione tra loro tramite strumenti diversi e canali non preordinati[12]. D'altronde è evidente come le tecnologie abbiano un impatto evidente sulla società[13], con un reciproco

---

intervenuta nel corso degli anni ad includere - nell'ambito della protezione assicurata dalla Carta citata - ogni forma di espressione, qualunque sia il mezzo di diffusione utilizzato, ivi compreso internet, e sottoponendo ad un accurato vaglio critico ogni intervento volto a limitare e condizionare tale libertà.

[8] «Internet è disegnata per muovere tutta l'informazione in maniera uguale, indipendentemente dal contenuto o dall'orientamento politico. La voce di un singolo cittadino può essere ascoltata alla stregua de più potente magnate dei media. Tutto questo è frutto della natura di Internet, pensata per connettere un numero enorme di punti in maniera efficiente. E la Rete è stata pensata per non avere un centro […] L'architettura della Rete riflette quindi i vecchi sogni della democrazia. Tutte le persone sono uguali. Tulle le idee hanno le stesse opportunità. Le barriere alla partecipazione civile sono state abbassate». D. WEINBERGER, "*Internet è libertà*", Il Sole 24 Ore, 11 marzo 2010.
In questo senso molti commentatori hanno descritto l'attuale società come "società della conoscenza", intendendo con tale espressione la possibilità di accedere alle varie fonti, elaborare il materiale reperito, diffondere liberamente le informazioni al fine di informare ed essere informati. Al riguardo l'art. 19 della Dichiarazione universale dei diritti dell'uomo delle Nazioni Unite (10 dicembre 1948) stabilisce il diritto di ogni individuo alla libertà di opinione e di espressione «e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere».

[10] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004. Si vedano anche, E. CUCCODORO (a cura di), *Libertà e comunicazione*, Roma, 2002. L. CORCHIA, *La democrazia nell'era di Internet: per una politica dell'intelligenza collettiva*. Vol. 66, *DiSPeS Unipi*, 2011; F. CARLINI, *Internet, Pinocchio e il gendarme: le prospettive della democrazia in Rete*, Roma, 1996; D. DE KERCKHOVE - A. TURSI, eds., *Dopo la democrazia?: il potere e la sfera pubblica nell'epoca delle reti*, Roma, 2006; J.M. BALKIN, *Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society*, in *New York University Law Review*, Vol. 79, 1/2004.

[11] Tale espressione indica una società moderna che, giunta al culmine del processo di industrializzazione, deve, per continuare a crescere, concentrare i propri sforzi verso la produzione non più di beni materiali bensì di servizi immateriali. D. BELL, *Thinking ahead*, in *Harvard Business Review* 57.3, 1979, 20-42; D. LYON - P. IELASI. *La società dell'informazione*. Bologna, 1991; A. MATTELART, *Storia della società dell'informazione*. Torino, 2002; C. BASILI, *La Società dell'Informazione*, in *Information literacy: un concetto solo statunitense?, AIDA Informazioni: rivista di Scienze dell'informazione* 19.2, 2001; W.H. JR. FORREST, *Information literacy vs. computer literacy,* in *American Society for Information Science Bulletin*, 9, April 1983, 14-16.

[12] C. SHIRKY, *Political Power of Social Media-Technology, the Public Sphere Sphere, and Political Change*, in *The Foreign Aff.* 90, 2011, 28.

[13] Secondo Milad Douehi la devozione nei confronti del digitale ha una natura quasi religiosa e la democrazia passa anche dal Web a patto che i cittadini continuino a vigilare e diventino utenti attivi sulle Rete, evitando l'appiattimento che deriva dalla "cultura passiva" che li porta a subire le nuove tecnologie piuttosto che a farne un uso consapevole. M. DOUEIHI, *Pour un humanisme numérique*. Paris, 2011.

condizionamento[14]. Tale mutamento ha assunto i caratteri di una vera e propria rivoluzione, che ha inciso profondamente sul tradizionale sistema delle comunicazioni, mutando i tratti essenziali della stessa dinamica politica.

Di fatto internet si è progressivamente imposta come "*il mezzo piú rapido e continuativo di consultazione, informazione e contatto tra cittadini e quindi di maggiore partecipazione alla vita democratica*"[15], così contribuendo ad avviare un processo universale e pervasivo di trasformazione della stessa democrazia rappresentativa verso una democrazia diretta deliberativa.

Dall'analisi dei processi che includono e valorizzano l'opinione dei cittadini, espressa mediante internet (*net-citizen*[16]) emerge infatti in modo crescente la tendenza a conferire rilevanza ai risultati dei processi deliberativi realizzati attraverso la Rete. Senza dubbio l'avvento dei nuovi *media* ha avuto l'effetto di indebolire fortemente i tradizionali centri di potere e gestione politica della comunicazione, riducendo il ruolo di interdizione degli intermediari e incoraggiando forme alternative di partecipazione.

Anche per la notevole riduzione dei costi dell'informazione, la Rete è uno strumento che consente ai cittadini, mediante rapide e periodiche consultazioni, di esprimere le loro preferenze su una molteplicità di questioni e di trasmetterle in modo semplice e immediato ai politici eletti, a livello nazionale e locale, con l'effetto di promuovere una maggiore partecipazione alla vita democratica[17] e con la

---

[14] Si tratta del principio di "*co-shaping*", influenza vicendevole. D.G. JOHNSON, *Computer Ethics*, Prentice Hall, 1985.

[15] Secondo Franco Gallo, ai partiti politici «[è] subentra[ta] quella che un apprezzato storico francese, Bernard Manin (Principi del governo rappresentativo, Bologna, 2010), chiama «la democrazia del pubblico» (audience democracy), in cui i partiti lasciano ampio spazio alla personalizzazione e la comunicazione, in qualunque modo realizzata, prende il posto dell'organizzazione: da una parte, le identità collettive, garanti della partecipazione, si indeboliscono e sono compensate dalla fiducia personale diretta; dall'altra, il rapporto con la società civile e con gli elettori passa sempre piú attraverso i media e il marketing politico. La differenza principale rispetto al passato è, dunque, che i partiti – nell'attuale situazione di disorientamento politico di massa – sono anzitutto al servizio di un leader o di un candidato. […] dietro questa svolta si nasconde il pericolo del populismo, ossia la tentazione di affidare i nostri destini ad un capo carismatico, che fa in continuazione promesse di salvezza. Nel libro quarto della Politica Aristotele scriveva che i populisti "criticano i magistrati sostenendo che giudice deve essere il popolo. Di conseguenza tutte le magistrature si sfasciano perché dove le leggi non governano non c'è costituzione. Ciò non vuol dire che la partecipazione politica sia inevitabilmente declinata insieme ai partiti di massa. Significa, più semplicemente, che la partecipazione istituzionale – in particolare quella elettorale – si è ridotta ed è stata sostituita da altre forme di partecipazione». F. GALLO, *Lectio magistralis* su: *Democrazia 2.0. La Costituzione, i cittadini e la partecipazione*, svolta a chiusura del Festival *Lector in fabula* organizzato dalla Fondazione Giuseppe Di Vagno. Conversano, 15 settembre 2013.

[16] Pertanto una delle ragioni precipue di insuccesso di tali esperimenti deliberativi è costituito dall'incapacità di tradurre la partecipazione dei cittadini in decisioni politiche concrete. S. COLEMAN - J. GOTZE. *Bowling together: Online public engagement in policy deliberation*, London, 2001.

[17] Tuttavia internet rimane pur sempre "uno strumento a vocazione minoritaria, elitario e "difficile", in quanto presuppone un ruolo attivo dell'utente nella ricerca delle informazioni" e "la ricerca della "controinformazione" su internet è spesso faticosa, richiede tempo e capacità di selezionare le fonti più affidabili, richiede quindi un utente avvertito, consapevole ed impegnato che abbia a

conseguenza che, come rileva Angelo M. Petroni, "*lo stesso processo di produzione legislativa viene ad essere radicalmente modificato*"[18]. La comunicazione politica diventa così interattiva[19], mediante referendum dai costi ridotti, che da strumento abrogativo di limitato utilizzo, può diventare mezzo a cui fare ricorso frequentemente, suscettibile di modificare non solo le modalità del processo di elaborazione delle leggi, ma il loro stesso contenuto[20].

Internet ha decentralizzato i processi informativi, sdoganando l'aura d'inaccessibilità che ammantava le autorità pubbliche, e la "globalizzazione comunicativa" ha accresciuto la trasparenza delle istituzioni, favorendo, almeno apparentemente, la collaborazione tra i diversi organismi politico-amministrativi[21].

Come rilevato, non vi è libertà senza regole*,* nel mondo *online* come in quello *offline.* In assenza di un quadro di regole puntuali ed efficaci che disciplinino compiutamente le modalità con cui si estrinsecano le manifestazioni dei cittadini sulla Rete, e la loro declinazione all'interno dei processi deliberativi, il superamento dei meccanismi consolidati di democrazia rappresentativa (che pure – come rilevato - può trovare in Internet gli elementi e gli stimoli per una proficua rigenerazione) si rivela illusorio e di difficile realizzazione. Ciò, in particolare, alla luce della concreta possibilità che le manifestazioni di volontà diffuse nel cyberspazio sia oggetto di manipolazioni e strumentalizzazioni.

Proprio nell'ottica di valorizzare internet come strumento e veicolo di libertà e conoscenza, regole e procedure si pongono come fondamentali strumenti di garanzia e tutela dei diritti nella Rete. E' ad essi che è affidato il compito di provvedere alla tutela del diritto di informare e essere informati, garantendo al contempo la sicurezza delle persone e degli Stati[22].

---

disposizione del tempo e abbia la capacità di cercare e selezionare le notizie». Il che mette in luce i rischi e le ambiguità del mito di una democrazia senza intermediari, che si traduce in ultima analisi nella dissoluzione e ridefinizione dello stesso concetto di cittadinanza. Così M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione*, Milano, 2008.

[18] A. M. PETRONI, *Trasformazione della democrazia rappresentativa,* Beltel, 2000.

[19] F. CAMPANTE - R. DURANTE - F. SOBBRIO, "*Politics 2.0: The Multifaceted Effect of Broadband Internet on Political Participation"*, RWP13-014, May 2013.

[20] Esempi di democrazia digitale sono rappresentati dalle *Consensus conferences,* dai *Town meeting* del New England, dalle Assemblee pubbliche che governano l'85% delle municipalizzate svizzere, dalle giurie civiche di Berlino, alla consultazione pubblica aperta nel 2007 dal governo neozelandese sulla riforma del corpo di polizia, fino alle iniziative legislative popolari a firma elettronica promosse dal governo finlandese nel 2013.

[21] J. FOUNTAIN, *Building the Virtual State: Information Technology and Institutional Change*, Brookings Institute Press, Washington D.C., 2001.

[22] Così F. GALLO, *supra* nota 15. Alcuni commentatori, al contrario, teorizzano la preminenza della libertà sulla Rete rispetto alla tutela dei diritti. Si veda, J. P. BARLOW, febbraio 1996. Inoltre, G. TEUBNER, afferma che la regolamentazione della Rete dovrebbe essere solo il frutto della stessa società civile e delle dinamiche sociali ed economiche da essa prodotte, dalle quali dovrebbero emergere "costituzioni civili" che prevalgono come fonte normativa sui tradizionali poteri politici e costituzionali. GALLO nota come secondo TEUBNER queste forme di autoregolamentazione dovrebbero superare la logica politica degli Stati per imporre nella sostanza il dominio dei regimi privati globali, portatori degli interessi settoriali del mercato. Il rischio dell'autoregolamentazione del cyberspazio

La società dell'informazione costituisce peraltro il terreno di scontro tra *hard law* e *soft law*, ma anche tra etica e diritto. Ai limiti dei tradizionali strumenti giuridici si affianca peraltro la riflessione secondo cui "*l'autoregolamentazione sarebbe comunque preferibile a regole imposte dall'esterno, che avrebbero un carattere autoritario o almeno paternalistico*". In quest'ottica parrebbe che la *soft law* rappresenti lo strumento maggiormente adatto a disciplinare una società dinamica quale quella attuale[23], o quantomeno suscettibile di affiancarsi alle regole giuridiche tradizionali.

Occorre quindi evitare di inseguire il facile mito di una democrazia senza intermediari che giunge a definitivo compimento grazie a internet; al riguardo devono soccorrere regole e procedure in grado di garantire valore alla partecipazione sulla Rete e consentire un dibattito reale e immune da semplificazioni, distorsioni, talora manipolazioni comunicative che rischiano di soffocarlo[24].

---

consta infatti nella probabile concentrazione del potere di gestione e controllo, anche politico, in capo a società multinazionali e a pochi Stati dominanti, i quali avrebbero così il vantaggio di strumentalizzare a loro favore le manifestazioni di volontà veicolate su Internet. F. GALLO, *Lectio magistralis* su: *Democrazia 2.0. La Costituzione, i cittadini e la partecipazione*, svolta a chiusura del Festival *Lector in fabula* organizzato dalla Fondazione Giuseppe Di Vagno. Conversano, 15 settembre 2013. Sul punto anche S. RODOTÀ, *Una costituzione per Internet*, in *Politica del diritto*, 2010, critica gli appelli ad un'indiscriminata libertà e autoregolamentazione della Rete, parlando di possibile "medioevalismo istituzionale". Sul ruolo della *corporations* e il rapporto con la diffusione dei valori democratici su Internet, si veda L. LESSIG, *The Internet under siege*, in *Foreign Policy*, 2001, 56-65.

[23] Secondo Gallo non risulta «[…] accettabile affidare alle multinazionali informatiche il futuro dei diritti politici, civili e sociali nel mondo virtuale del cyberspazio. Se si seguisse la via della spontanea autoregolamentazione […], si correrebbe infatti il rischio di concentrare i poteri e le risorse nelle mani delle società multinazionali e degli Stati dominanti, i quali avrebbero cosí il vantaggio di utilizzare Internet solo per i propri interessi. […] Sarebbe come lasciare la tutela dei diritti in Rete solo all'iniziativa dei soggetti privati, i quali, in assenza di altre iniziative, appariranno come le uniche istituzioni capaci di intervenire. Sarebbe, in particolare, come accettare una privatizzazione del governo di Internet senza che altri attori, ai livelli piú diversi, possano dialogare e mettere a punto regole comuni. Dice bene G. Azzariti (Internet e Costituzione, 18 febbraio 2011) che in questa situazione tutto avverrebbe, meno che configurare una cittadinanza elettronica democratica. […] Per evitare questi risultati non resta, quindi, che prendere atto che viviamo ancora in un'epoca tecnologica in cui manca una disciplina super partes che garantisca con pienezza, senza discriminazioni e a livello planetario, i diritti fondamentali di informazione dei cittadini e le libertà degli utenti. Ed occorre anche prendere atto che la questione della democrazia di internet può essere risolta solo costituzionalizzando la Rete nel senso di porre tali diritti fondamentali al centro del potere informatico degli Stati e delle *corporations*. Il che – lo ripeto – dovrebbe avvenire non affidandosi alle regole spontanee del mercato, ma regolando tali diritti e tali libertà con norme costituzionali sia statali sia sovranazionali. […] Il fatto è che, se non si introdurrà in futuro una soddisfacente regolamentazione del cyberspazio su base transnazionale, transgenerazionale e non ideologica, difficilmente la Rete potrà costituire un sicuro spazio di libertà e si presterà, anzi, sempre piú a manipolazioni e distorsioni comunicative». F. GALLO, *Lectio magistralis* su: *Democrazia 2.0. La Costituzione, i cittadini e la partecipazione*, svolta a chiusura del Festival *Lector in fabula* organizzato dalla Fondazione Giuseppe Di Vagno. Conversano, 15 settembre 2013.

[24] L. MOSCA - S. TARASSI, *Le campagne elettorali online*, Bologna, 61.6, 2012, 1118-1125; L. MOSCA, *Le campagne elettorali online fra innovazione e manipolazione*, in *Parolechiave* 20.1, 2012, 95 ss.

L'esperienza dimostra come la Rete, strumento prezioso e strumentale al godimento di diritti (*inter alia*, il diritto all'educazione, ad informare ed a essere informati), talora presenta profili delicati. Si pensi per esempio alla tendenza, evocata da taluni autori, verso l'omologazione e omogeneizzazione[25] della conoscenza *on-line* in conseguenza di quelli che Eli Pariser ha definito *bubble filter*, di siti che confezionano informazioni a misura dell'utente, proponendo un risultato di ricerca[26] che non è quello effettivo, bensì quello basato su un algoritmo che genera "universi di informazione" a sé stanti diversi per ciascuno[27], una sorta di realtà a nostra immagine e somiglianza.

A ciò si aggiunge il rischio crescente della cosiddetta "minaccia ibrida", vale a dire vale a dire campagne mirate di disinformazione poste in essere con per o più non convenzionali, insidiose e difficili da contrastare in quanto in continua evoluzione, che incidono infatti sull'opinione pubblica e la rendono vulnerabile, alterando i meccanismi di formazione del consenso e lo stesso processo democratico. Loro strumento precipuo sono i *Social Network*, ormai considerati ambienti virtuali rilevanti ai fini della sicurezza nazionale e dei relativi interessi strategici, piattaforma ideale per l'avvio di attacchi condotti sovente da paesi terzi attraverso *hackeraggio* di reti, tecniche che comprendono la manipolazione di video o documenti ufficiali, *bot e troll,* campionario di una nuova *warfare* non meno cruenta di quella tradizionale.

Contro l'utopia che la tecnologia possa risolvere da sola questioni complesse (la "*nerd supremacy*") si rivolgono coloro che segnalano come sia illusorio ritenere che la grande quantità di dati disponibile *online* porti automaticamente alla trasparenza e alla verità[28].

Altro rischio è quello insito nella concentrazione del potere economico[29] in capo a una manciata di multinazionali, aspetto che appare di particolare rilievo se si tiene

[25] J. LANIER - N. CARR sottolineano l'attuale tendenza verso una omogeneizzazione della conoscenza *on-line*, in cui Internet sta diventando un "supermercato della conoscenza", ove le posizioni più conformiste prevalgono e la discussione è condizionata da operatori dominanti e siti Web. Il rischio paventato è che il presunto egualitarismo del Web stia diventando ormai una sorta di dittatura della massa.
J. LANIER, *Tu non sei un gadget,* Milano, 2010, 6; N. CARR, *Il lato oscuro della Rete: libertà, sicurezza, privacy*, Milano, 2008.

[26] In base ad un processo che ha una durata di poche frazioni di secondo, l'utente inserisce una parola, il sistema estrae documenti rilevanti per la ricerca, li analizza ed elabora una gerarchia prima di restituirli, grazie al costante lavoro di catalogazione dei "ragni" informatici che giorno e notte esplorano il Web. AMY N. LANGVILLE - CARL D. MEYER , *Google's PageRank and Beyond: The Science of Search Engine Rankings*, 2012.

[27] Eli Pariser afferma che Internet sta diventando sempre più una "cassa di risonanza" in cui i siti Web confezionano le informazioni su misura in base alle preferenze che individuano in ogni spettatore. E. PARISER, *Il filtro. Quello che internet ci nasconde*, Milano, 2012.

[28] Si veda J. LANIER, *The hazards of Nerd supremacy*, The Atlantic, 20 dicembre 2010, L. LESSIG, *Against transparency*, New Republic, 9 ottobre 2009.

[29] "In primo luogo, le caratteristiche proprie dei mercati in esame (effetti di Rete, rendimenti di scala, *multi-homing* e *switching cost*, ecc.) facilitano, come detto, l'emergere di equilibri caratterizzati da un elevato livello di concentrazione (se non addirittura da un esito quasi monopolistico, cd. the

conto che la tecnologia moderna è costituita da strumenti tecnici che si esplicano sulla base del cosiddetto *any approach*: vale a dire, un'offerta di servizi *media* in "qualsiasi" tempo e luogo, da "qualsiasi" mezzo di ricezione, fornita ad una generalità di utenti a diversi livelli di interattività, capace dunque di influenzare in modo radicale gli individui e la società[30] . L'esperienza mostra infatti che vi è una tendenza naturale alla concentrazione delle risorse nei mercati delle comunicazioni; il che comporta, evidentemente, la necessità di mantenere un ambiente pluralistico e competitivo, vagliando con cura le inevitabili operazione di aggregazione e concentrazione fra imprese anche in relazione ai nuovi canali di distribuzione, per i media tradizionali sia per quelli più innovativi.

Considerata l'importanza che oggi rivestono i dati, risulta necessario aggiornare con rapidità gli strumenti *antitrust* perchè possano essere applicati ad un mercato digitale ormai saldamente in mano a cinque colossi: Alphabet (la società madre di Google), Facebook, Apple, Amazon e infine Microsoft, sopravvissuto al passaggio dalla terza alla quarta rivoluzione industriale. Significativo il fatto che metà del denaro speso *on line* finisca ad Amazon, mentre Google e Facebook incamerano gran parte delle risorse derivanti dalla raccolta pubblicitaria del settore digitale.

E' stato il New York Times ad aprire il 22 aprile 2018, con un titolo ad effetto: "*Is time to break up Google*?", il dibattito sull'opportunità di adottare drastiche misure di deconcentrazione e dismissione. Si tratta di quelle che ai primi del novecento negli Stati Uniti avevano riguardato *Standard Oil* o, più di recente, AT&T nel settore delle telecomunicazioni, oppure quelle che in Europa all'inizio degli anni '90 avevano aperto alla concorrenza, con il supporto della Corte di Giustizia, il mercato delle *public utilities* (telecomunicazioni, energia, trasporti) con un incisivo intervento sulle *essential facilities* volto a rimuovere tutti i "colli di bottiglia" anticoncorrenziali.

---

winner takes all). Ciò determina un primo elemento di criticità concorrenziale, proprio in ambiti di mercato (a monte, sistemi operativi e browser, a valle, motori di ricerca e *social network*) che rappresentano degli snodi cruciali per l'intero assetto competitivo dell'ecosistema di Internet. Si è visto ad esempio come almeno più di un terzo del traffico complessivo dei siti di *news online* provenga da motori di ricerca e *social network*. […]. Ad un secondo livello, le maggiori piattaforme di servizi Web stanno aggregando sempre più servizi al loro interno attraverso una strategia di *platform envelopment*, che presuppone la presenza in vari stati della filiera produttiva del Web, nonché, in via strumentale, la creazione di potenti reti di server dislocate in tutto il mondo. […]. L'insieme dei due fenomeni rende opportuna non solo un'attenta attività di monitoraggio dei mercati, ma anche una rigorosa verifica delle condizioni di interoperabilità delle piattaforme. Solo l'interoperabilità dei servizi è, infatti, idonea, almeno in prima battuta, a ridurre le barriere all'ingresso nei mercati, moderando gli effetti concentrativi delle esternalità di Rete, nonché le economie di varietà derivanti dal bundle di servizi Web". AGCOM, *Indagine conoscitiva sul settore dei servizi internet e sulla pubblicità online*, Allegato A alla Delibera n. 19/14/CONS del 21 gennaio 2014, pt. 643 ss.

[30] Si veda in questo senso Gladwell, il quale elabora il concetto di *slacktivism*, attivismo pigro, che induce a spesso a "postare sulla Rete", senza poi preoccuparsi dell'effetto positivo o negativo dell'intervento svolto, M. GLADWEL, "Small change, why the devolution will not be tweeted", The New Yorker, 4 ottobre 2010, E. MOROZOV, *From slacktivism to activism*, in *Net Effect, Foreign Policy,* 2009, C. JONES - W. KENT, *Activism or Slacktivism? The Role of Social Media in Effecting Social Change*, in *Research Paper. School of Engineering and Applied Science: University of Virginia*, 2013.

Avere dimensioni rilevanti per un'azienda non è certo una colpa ma "*in una società democratica l'esistenza di vasti centri di potere privati è pericoloso per la vitalità di un popolo libero*", come rilevava all'inizio del secolo scorso Louis Brandeis, giudice della Corte Suprema USA.

In effetti molto è cambiato rispetto a qualche anno fa: la gran quantità e varietà dei dati in circolazione ha cambiato la natura stessa della competizione fra imprese, la cui verifica deve essere svolta con metodi, strumenti e rimedi adeguati ed efficaci.

I giganti della tecnologia hanno sempre beneficiato di economie di scala e dei "*netwok effects*" (più Facebook ha iscritti, più diventa più interessante per gli altri iscriversi al servizio), ma il loro potere è andato ben al di là una mera dominanza economica per coinvolgere delicati profili che attengono all'accesso all'informazione e incidono sugli stessi meccanismi di formazione del consenso. Tutto ciò in virtù del potere dei dati, che consegna il mercato a chi ne abbia controllo e capacità di analisi (Google vede quello che le persone cercano, Facebook quello che condividono, Amazon quello che comprano) e consente di giocare d'anticipo rispetto alle mosse dei concorrenti. Come rilevato dalla Commissione europea nei recenti casi WhatsApp/Facebook e Microsoft/Linkedin, non si può generalizzare perché i dati non sono tutti uguali (dati grezzi o replicabili dagli altri concorrenti non attribuiscono di norma significativi vantaggi). Tuttavia un mercato condizionato da barriere all'ingresso e da un sistema di *early warning* quale quello delineato impone un deciso salto di qualità, da parte di regolatori e autorità antitrust. Al riguardo, un esempio lo fornisce il legislatore tedesco che ha recentemente introdotto il possesso di dati quale elemento da considerare nel controllo delle concentrazioni così da rendere possibile lo scrutinio di operazioni che, altrimenti, solo sotto il profilo economico non superebbero le soglie di rilevanza economica.

E' sempre più diffusa la convinzione che l'utilizzo sempre più diffuso degli algoritmi, a vari livelli e in diversi settori, presenti il rischio di decisioni discriminatorie e irragionevoli, laddove non si conoscano (e non si riescano a disciplinare) i meccanismi posti alla base dell'effettivo funzionamento della "scatola nera".

Di qui l'iniziativa assunta dal Parlamento britannico di invitare il governo a prendere iniziative in merito. In un rapporto su: "*Algorithms in decision-making*" pubblicato il 23 maggio 2018, il Comitato "Scienza e tecnologia" della Camera dei Comuni ha rilevato come la tecnologia debba essere utilizzata per migliorare la qualità dei servizi pubblici e guidare l'innovazione, in particolare in settori come i trasporti e la sanità. Alla base di tutto vi sono i dati, soprattutto quelli in mano al settore pubblico, sui quali operano algoritmi complessi a cui non ci si può affidare senza pretendere il rispetto di una serie di regole, anche di carattere etico. In sostanza, il Rapporto evidenzia che l'applicazione degli algoritmi, al pari di ogni decisione umana, può talora essere condizionata da errori che comportano esiti imprevedibili e talora discriminatori, soprattutto nei confronti di determinate categorie sociali, se è alterato o non correttamente gestito il loro funzionamento.

Per evitare tale rischio, il governo è stato invitato ad affidare al "*Centre for Data Ethics and Innovation*" (DEI)[31], organismo consultivo previsto dalla legge di bilancio del 2017 e poi istituito nell'ottobre 2018, il compito di verificare il funzionamento degli algoritmi. Il che significa controllare la qualità dei dati sui quali gli stessi si basano assicurandosi che i loro sviluppatori siano in grado di spiegare come funzionano. Tali meccanismi dovrebbero infatti essere pubblicati e conoscibili a tutti, nel momento in cui incidono sui diritti e la libertà dei cittadini.

Il tema della trasparenza dell'algoritmo è peraltro diventato centrale soprattutto alla luce del regolamento europeo 2016/679, che introduce il concetto della "correttezza e trasparenza" dei dati, vale a dire la disponibilità di strumenti in grado di verificarne l'affidabilità, quali per esempio accurati sistemi di audit per gli algoritmi e di certificazione per i loro sviluppatori, come raccomandato dal Comitato della Camera dei Comuni. Potrebbero al riguardo essere previsti dei "*data trusts*", metodo ipotizzato nel rapporto sull'intelligenza artificiale presentato al governo nel 2017 dallo scienziato Wendi Hall e dall'amministratore delegato di BenevolentTech Jérôme Pesenti. L'idea è in sostanza di prevedere modalità standardizzate a beneficio delle entità che gestiscono dati che intendono condividere.

Il Comitato ha richiesto poi al governo di preparare un elenco, accessibile al pubblico, dei casi in cui sono usati gli algoritmi che hanno "*un impatto significativo*" o di cui il governo centrale prevede l'utilizzo, così da accrescere la trasparenza e incoraggiare il coinvolgimento anche del settore privato. A ciò si aggiunge la necessità di istituire un "*champion*" nazionale, di rango ministeriale, in grado di vigilare sugli algoritmi usati nel settore pubblico e coordinare i vari dipartimenti interessati. E' poi posta una particolare enfasi sulla cooperazione internazionale, la necessità che l'*Information Commissioner's Office* (ICO), il garante per la privacy britannico, disponga di adeguate risorse finanziarie e che sia sempre pubblicata e disponibile la valutazione d'impatto sulla protezione dei dati personali prevista dal Regolamento europeo. Insomma, svariate iniziative meritevoli di attenzione.

Una regolamentazione saggia e lungimirante del cyberspazio deve dunque tener conto dei molteplici caratteri di internet che, proprio come un *Giano bifronte*, è suscettibile di assumere *valenze* diametralmente opposte. Occorre un cyber-realismo per indurci a beneficiare appieno della Rete senza cadere nei pericoli insiti in un mezzo potente e per lo più incontrollabile, dalla memoria infallibile,

Obiettivo da perseguire è pertanto quello di delineare una cornice giuridica, a vari livelli, che garantisca il rispetto dei diritti e della liberta individuale, nella quale le nuove tecnologie non portino ad una concentrazione del potere sociale e politico basata sulla sorveglianza, bensì ad una sua diffusione[32]. Soltanto in tal modo si può garantire che internet non degradi a strumento di controllo, diffusione e amplificazione delle disuguaglianze ma continui ad essere veicolo di conoscenza,

[31] Il DEI ha pubblicato il suo ultimo rapporto su "*Online targeting*" il 20 febbraio 2020.

[32] Sull'uso strategico della Rete si veda F. VITALI, *La geopolitica economica dei dati e il futuro del dominio,* Nomos & Khaos, Roma, 2012, 207.

libertà, promozione umana, e che il potenziale creativo delle nuove tecnologie accresca le possibilità di confronto aperto fra idee, per una conoscenza libera e pluralista, evitando forme insidiose di privatizzazione dell'informazione.

Nel documento di lavoro "*Six Ideas for Rejuvenating European Democracy - Strengthening Digital Democracy*" del novembre 2019, Carnegie Europe segnala che occorre sfruttare il potenziale degli strumenti digitali e mitigare i possibili rischi, a tutela della democrazia. Negli ultimi anni questo è avvenuto soprattutto mediante gli strumenti della regolazione (il regolamento 2019/679 *in primis*). In vista delle elezioni europee del maggio 2019 l'UE ha indotto aziende come Facebook, Google, e Twitter ad adottare un codice di buone pratiche contro la disinformazione (con l'impegno delle tre piattaforme firmatarie a riferire mensilmente sulle azioni intraprese per garantire trasparenza politica e agire contro gli account falsi e l'uso nocivo dei malware (bot). Tuttavia – rileva Carnegie Europe - l'Unione europea dovrebbe sfruttare il potenziale positivo delle innovazioni digitali per migliorare la qualità della democrazia, come è avvenuto in Finlandia, Lituania, Lussemburgo, Slovenia, Estonia e Islanda, ove petizioni elettroniche e piattaforme digitali online hanno dato voce ai cittadini, favorito una più stretta interazione con i loro governanti e consentito loro di influenzare il processo decisionale, così rafforzando la legittimità del sistema.

1.3 Intelligenza artificiale e controllo in Cina. Un sistema distopico

1.3.1. Sovranità digitale alla cinese

Al contrario dell'evoluzione in corso in Europa, in Cina il concetto di "sovranità digitale", una delle parole d'ordine dell'élite politica cinese negli ultimi anni, sta assumendo un significato nuovo e forse non del tutto previsto.

In base alla legge sulla cybersicurezza approvata nel giugno 2016, Apple è stata costretta a rimuovere dal suo *store* cinese tutte le applicazioni, divenute assai popolari, che consentono agli utenti di bypassare il "*Great Firewall*". Si tratta delle reti VPNs (reti private virtuali) di solito usate da stranieri, società multinazionali e da molti cittadini cinesi per accedere a indirizzi quali Gmail, Google, Facebook (le applicazioni vendute attraverso lo *store* di Apple sono peraltro le sole disponibili) il cui accesso é bloccato o rallentato. Come rileva il Financial Times il 1° agosto 2018, Pechino persegue un obiettivo chiaro: chiudere tutte le reti VPNs senza licenza.

Appare paradossale che, a fronte dell'insistenza del Presidente Xi Jinping sulla necessità di sviluppare il digitale, il modello di regolazione previsto rischi di isolare la Cina nel sistema dell'internet globale, ponendo altresì tutti coloro che hanno a che fare con la seconda economia del pianeta di fronte ad una serie di rischi. L'approccio adottato nei confronti di Apple potrebbe infatti avere come conseguenza che, per esempio, i manager presenti nel paese non siano più in grado di ricevere messaggi o accedere ad informazioni importanti per il proprio lavoro.

Un altro problema, non meno rilevante, è quello delle regole per la protezione dei dati personali. Se gli utenti sono obbligati ad accedere dall'estero a siti usando reti VPNs fornite da ISP ufficiali cinesi, non vi è alcuna garanzia che l'apparato di

sicurezza di Pechino non raccolga segreti commerciali o informazioni confidenziali. Non sorprende dunque che ExpressVPN, che vende una delle applicazioni rimosse, abbia rimproverato alla società statunitense di aver accettato la censura imposta dal governo cinese. In realtà Apple non aveva scelta, poiché il Ministro dell'industria e dell'informazione tecnologica aveva annunciato qualche mese prima che tutte le VPNs avrebbero dovuto disporre di una licenza locale, salvo esporsi alle incognite di un contenzioso legale.

Dalla vicenda emerge dunque una concezione piuttosto discutibile di sovranità digitale, che di fatto disconosce l'importanza del libero flusso delle informazioni in un sistema di scambi globali. Tutto ciò mentre giganti cinesi come Alibaba e Tencent si espandono negli USA e in Europa. Vani si sono rivelati finora gli inviti rivolti alla Cina a sottoscrivere un codice di comportamento condiviso sulle libertà digitali tale da salvaguardare e garantire un accesso alla Rete senza discriminazioni o controlli indebiti.

1.3.2. Riconoscimento facciale e sicurezza interna

Significativo il caso dei sistemi di riconoscimento facciale, che da strumento contro la criminalità pare ormai essere diventato funzionale all'esercizio di poteri di sorveglianza globale, secondo quanto riportato da Bloomberg il 17 gennaio 2019 con riferimento alla regione cinese del Xinjiang, la frontiera ovest del Paese al confine con l'Afghanistan e il Pakistan, i cui villaggi ospitano circa 10 milioni di musulmani di etnia Uigura, che è diventata una sorta di laboratorio in cui si applicano tecnologie per il controllo di ampie fasce di popolazione.

Su impulso del Presidente Xi Jinping, intenzionato a liberarsi dei terroristi islamici autori di attacchi efferati nel 2013 e 2014, compresi quelli alle stazioni ferroviarie di Guangzhou e Kunming, la regione è diventata uno dei luoghi più diffusamente controllati al mondo, con una presenza capillare di forze di polizia e un sistema sperimentale che invia un segnale di allarme se le persone si allontanano per più di 300 metri dalle cosiddette "zone sicure", che comprendono le abitazioni e i luoghi di lavoro. In effetti in tutta la regione sono presenti numerosi posti di blocco, stazioni di polizia e telecamere di sicurezza. Tutti devono sottoporsi a scansione facciale prima di entrare al mercato per fare la spesa, il pieno di carburante o prendere una corriera. Il sistema di sorveglianza ha iniziato ad essere testato all'inizio dello scorso anno e riguarda soprattutto la parte meridionale della regione ove si trova Kashgar, importante nodo logistico per gli scambi commerciali Europa-Asia, parte integrante del "*Belt and Road Initiative*".

Il riconoscimento facciale è ormai strumento essenziale del programma di sorveglianza nazionale a cui il governo due anni fa ha dato impulso, chiamato "Xue Liang" (in cinese, potere di controllo globale), che pone la Cina all'avanguardia dal punto di vista tecnologico. E' gestito da *China Electronics Technology Group*, società statale del settore della difesa che ha sfruttato le proprie competenze nel settore spaziale e dei sistemi radar per dedicarsi alla sicurezza interna e sviluppare un *software* per raccogliere dati su attività professionali, hobbies, abitudini e comportamenti dei cittadini con l'obiettivo di prevedere crimini prima che siano

commessi. La Cina rappresenta ormai il 46 per cento del mercato globale della sorveglianza video e tre quarti dei servizi di "*deep learning*" per l'analisi dei dati, secondo Jon Cropley, analista di IHS Markit; nel 2015 ha stanziato per la sicurezza interna la somma record di 146 miliardi di dollari, più di quanto abbia fatto per la difesa militare. D'altronde, il controllo sulla regione dello Xinjiang, più vicina a Bagdad che a Pechino, è una preoccupazione del potere centrale cinese sin dal tempo degli imperatori e l'attuale governo accusa i separatisti che non riconoscono la sovranità cinese di fomentare rivolte e terrorismo. Di qui gli sforzi per elevare il livello della risposta tecnologica per salvaguardare – così si è espresso l'anno scorso il Presidente cinese - la sicurezza nazionale e la stabilità sociale.

Questo evidentemente non fa che alimentare le preoccupazioni di Stati Uniti e Unione europea sul rispetto della liberta di circolazione e dei diritti delle minoranze etniche anche perché – come rileva Jim Harper del *Competitive Enterprise Institute* - un tale sistema di controllo generalizzato, che peraltro è assai poco costoso, ha l'effetto di comprimere i diritti e condizionare la libertà d'azione dei cittadini, perché chi sa di essere costantemente controllato non è libero.

1.3.3. La sorveglianza emozionale

La retorica esortazione: "*Se non hai nulla da nascondere non hai nulla da temere*" rivolta dal governo britannico all'opinione pubblica, alla ricerca del consenso per introdurre rigide misure di sicurezza all'indomani degli attacchi terroristici alla metropolitana di Londra del 2005, pare oggi ingenua e anacronistica in confronto a quanto si sta verificando in Cina, ove in poco tempo è stato dispiegato un sistema di sorveglianza globale senza precedenti, che azzera ogni residuo spazio di libertà individuale.

La strenua competizione tra Cina e Stati Uniti sul fronte dell'intelligenza artificiale (IA) si arricchisce infatti di un nuovo capitolo, quello del controllo delle emozioni, rilevate mediante una tecnologia applicata su larga scala, dal settore industriale alla difesa, dalla sanità al trasporto aereo.

Uno dei principali centri di ricerca è Neuro Cap, creato sulla base di un progetto governativo presso l'Università di Ningbo. La tecnologia per il programma di "sorveglianza emozionale", ideata per aumentare la competitività e mantenere la stabilità sociale mediante il controllo dello stato mentale degli individui, è stata finora applicata in diverse società e fabbriche per eliminare errori umani, evitare danni al ciclo produttivo e prevenire incidenti. Invisibili sensori, inseriti nei cappelli che indossano operai, piloti di aereo o militari, controllano costantemente i loro stati d'animo e inviano i dati ai computer che operano sulla base degli algoritmi dell'IA per rilevare ansia, depressione o rabbia. Quando il sistema registra per esempio fatica e calo di attenzione oltre certi limiti, da l'allarme e il supervisore impone il riposo forzato.

A ciò si aggiungono telecamere per il riconoscimento facciale diffuse pressochè ovunque. La polizia ferroviaria della provincia di Henan usa occhiali *smart* per controllare i passeggeri. Secondo l'agenzia di stampa statale Xinhua, una tecnologia

elaborata per i missili viene utilizzata per gli *scanner* corporali negli aeroporti, in grado di rilevare in un secondo 89 materiali vietati, comprese sostanze corrosive e liquidi infiammabili. Dal 1° maggio 2018 è entrato in azione un sistema di controllo dei volti dei guidatori per verificare la validità delle patenti di guida. In Cina si stima siano in azione circa 172 milioni di telecamere (tre volte quelle operanti negli Stati Uniti).

Il *South China Morning Post* del 17 febbraio 2018 riporta che a Pechino telecamere poste nei bagni pubblici accanto al Tempio del Paradiso individuano chi sottrae carta igienica mentre all'Università rilevano gli studenti che si annoiano a lezione. A Shenzhen, sede di società quali Tencent, Huawei e ZTE, oltre che di *start-up* note come DJI e BGI Genomics, sono sperimentate le più avanzate tecnologie per il controllo delle violazioni stradali, che sono in seguito anche esportate. La *start-up* Yitu Tecnologies ha da poco venduto alla polizia malese mini telecamere indossabili munite del *software* di riconoscimento facciale per identificare i sospetti criminali.

Le prime telecamere per il controllo della velocità lungo le strade sono state installate nel 1997, a cui hanno fatto seguito nel 2001 sistemi di sorveglianza per identificare anche di notte i numeri di targa delle auto. Da aprile 2017 le foto ad alta risoluzione dei pedoni negligenti sono trasmesse su mega schermi e gli stessi identificati grazie alle banche dati della polizia, ove tutti i residenti sono obbligati a registrarsi. Ai trasgressori viene contestata l'infrazione e irrogata l'ammenda tramite messaggi inviati sul cellulare. Il sistema è in grado di registrare quante volte il pedone ha violato in un determinato periodo le regole del traffico e, se è ripetutamente passato con il rosso, si vedrà decurtare il "credito sociale" con il rischio di vedersi poi negare il mutuo dalla banca.

La Cina ha qualificato quattro delle sue maggiori imprese tecnologiche, Baidu, Alibaba Group, Tencent Holdings e iFlyTek come "campioni nazionali" per guidare lo sviluppo delle piattaforme dell'IA, rispettivamente nelle auto a guida autonoma, *smart cities*, computer per diagnosi mediche e riconoscimento vocale. Il segreto del successo è nella combinazione di dati, algoritmi ed esperti e la forza della Cina risiede nell'enorme disponibilità di dati (gli utenti internet sono oltre 700 milioni, i cui dati sono raccolti e scambiati senza alcuna regola fra imprese private e autorità pubbliche).

Comprensibile che, a queste condizioni (nessuna norma a protezione dell'individuo, men che meno quelle in tema di privacy, completa privazione della libertà, nessun dibattito pubblico, investimenti smisurati), la strada verso il predominio cinese nell'IA - che vede per ora ancora saldamente in testa gli USA - sia destinata a non trovare ostacoli.

1.3.4. Intelligenza artificiale e controllo

In Cina Stato ed economia sono strettamente interconnessi e l'intelligenza artificiale diventa sempre più strumento precipuo di controllo sociale, così offrendo una rappresentazione inquietante del futuro che ci attende.

Alla periferia di Hangzhou, nella "Città delle Nuvole" di Alibaba, centro di lavoro e tempo libero, automazione e infrastrutture, costruita in stile Silicon Valley, si stanno sperimentando le tecniche più avanzate, ennesima dimostrazione che in Cina dimensione pubblica e privata, business e strategia governativa sono ormai strettamente integrati. Si tratta di semafori che in base al riconoscimento facciale identificano l'età del pedone concedendo maggior tempo all'anziano per attraversare la strada, auto munite di un pannello multimediale collegato allo *smartphone* del passeggero che ne rileva i movimenti pregressi, raccoglie e analizza tutti i suoi dati, registra le preferenze alimentari per indicargli in quale ristorante andare o come ordinare il cibo preferito. Il cittadino in tal modo esternalizza i desideri e li affida ad Alibaba per esaudirli. I suoi impulsi sono organizzati e pianificati in modo sistematico e la triangolazione tra dati, tecnologia predittiva e bisogni è alla base del funzionamento di una città talmente intelligente da suscitare inquietudine.

E' vero che tutto questo in realtà non è molto lontano dalla tecnologia di Google Now, sin dai progetti per la sua attuazione nel 2012. Il punto è che Alibaba può usare i suoi complessi algoritmi per privilegiare i punti vendita che usano Alipay piuttosto che quelli che usano WeChat Pay, per esempio. Allo stesso modo, se Google risponde alle domande del cittadino/consumatore che le abbia poste, lo indirizza ove non avrebbe neppure immaginato di andare.

Ci troviamo insomma nella fase iniziale di una rivoluzione tecnologica in cui il desiderio non è solo previsto, ma orientato e costruito per soddisfare esigenze all'interno di un processo con cui sono plasmati i bisogni e i sogni di un intero popolo che è funzionale non solo all'interesse economico di Alibaba ma a quello di un Stato sempre più invadente.

Tencent, altra importante società tecnologica, rivale di Alibaba e con stretti legami con il governo di Pechino, dispone della capacità di mappare il territorio rilevando il calore sprigionato dalle persone. Il che le permette di scoprire dove si sta formando una folla, consentendo alle autorità di prevenire le proteste di strada. Ma Alibaba pare focalizzata su strumenti ancora più raffinati che incidono sullo stesso processo cognitivo, per esempio sull'intenzione dei cittadini di manifestare, prima ancora che si traduca nella decisione di scendere in piazza. L'impressione è quella di un processo inesorabile verso un autoritarismo hi-tech in cui una società guidata dalle tecnologie sta plasmando i cittadini in senso conforme ai propri obiettivi.

1.3.5. La rete dei cavi sottomarini e l'attivismo cinese

La rete dei cavi sottomarini in fibra ottica costituisce un'importante infrastruttura critica. Costituisce la "colonna vertebrale" dell'internet globale, essenziale per il commercio e le comunicazioni internazionali, nuova frontiera della sicurezza. Lungo i cavi sottomarini scorrono gran parte dei dati e delle comunicazioni mondiali e una loro compromissione sarebbe devastante per la stessa società. Eppure la necessità di proteggerli identificando con rigore i potenziali rischi risulta un argomento piuttosto trascurato dal punto di vista strategico, a differenza di quanto avvenuto con la pirateria o gli attacchi informatici ai porti, per esempio.

Il rapporto dell'"Information Technology & Innovation Foundation" dell'aprile 2019, dedicato a "*Submarine Cables: Critical Infrastructure for Global Communications*" di Dough Brake illustra in modo approfondito il ruolo e le problematiche inerenti i cavi sottomarini per le reti interconnesse globali, che trasportano circa il 99% del traffico delle comunicazioni internazionali. Oggi i cavi sottomarini utilizzano la tecnologia a fibra ottica, per cui le informazioni sono codificate su onde di luce trasmesse dai laser attraverso sottili fibre di vetro e il loro utilizzo cresce in modo esponenziale per le applicazioni ad alta intensità di banda, come i video ed i servizi basati sul *cloud,* con un aumento medio, negli ultimi cinque anni, del 26% della capacità disponibile[33].

La loro origine risale al 1850, quando il primo cavo fu posato nel Canale della Manica per consentire le comunicazioni telegrafiche tra il Regno Unito e l'Europa continentale. Si tratta per lo più di beni privati, piuttosto costosi (fra i 100 e i 500 milioni di dollari) seppur non quanto la loro alternativa via satellite (si consideri per esempio il progetto in corso ad opera del consorzio industriale OneWeb Satellites, costituito dalle aziende Airbus e OneWeb, per un internet veloce basato su una serie di satelliti). I cavi sono posati in mare ad una velocità massima di 200 km al giorno da navi specializzate, in grado di trasportare fino a 2000 km di cavi. Nelle aree *offshore* vengono adagiati direttamente sul fondo del mare mentre, sulla piattaforma continentale, una sorta di aratro viene utilizzato per interrare i cavi e proteggerli dai danni accidentali, solitamente causati da ancoraggi.

E' in questo contesto che emerge l'attivismo della Cina, sia come fornitore attraverso Huawei Marine, sia come acquirente tramite società di comunicazioni statali che comprano cavi in consorzio. Gli attori cinesi partecipano anche a progetti di finanziamento in infrastrutture con la China ExIm Bank, che finanzia diversi progetti nei paesi in via di sviluppo. Protagonista è la società Huawei Marine, *joint venture* fondata nel 2008 tra Huawei (51%) e una controllata della britannica Global Marine Systems (49 %), attiva in tutto il mondo, in particolare in Africa. Questa rapida espansione delle aziende cinesi a livello globale, insieme alla presenza dominante di Huawei nelle reti 5G e al quadro regolamentare al quale sono sottoposte, con la presenza costante del governo cinese, suscita il timore di possibili rischi per le vulnerabilità di sicurezza, la raccolta e il trasferimento indebito di informazioni critiche[34].

Si tratta delle preoccupazioni per la sicurezza informatica ed i possibili rischi di spionaggio[35] che hanno indotto, per esempio, l'intelligence australiana ad annullare il progetto di Huawei per collegare le Isole Salomone a Sydney. A ciò si aggiungono le contestazioni dei concorrenti secondo cui Huawei Marine riceverebbe sussidi dal governo cinese che le consentono di vendere sottocosto e offrire incentivi per i

[33] Così W. Nielsen, "*Submarine Telecoms Industry Report, 7th Edition*" Submarine Telecoms Forum, 2019.

[34] J. Page e al., "*America's Undersea Battle With China for Control of the Global Internet Grid*", *Wall Street Journal*, marzo 2019.

[35] S. Lee, "*The Cybersecurity Implications of Chinese Undersea Cable Investment*" *East Asia Center, University of Washington,* febbraio 2017.

contratti[36]. Vero è che diversi progetti a cui Huawei ha partecipato sono stati finanziati dalla Bank of China. Occorre peraltro rilevare che Huawei Marine dispone finora di una ridotta quota del mercato globale, focalizzata su progetti più limitati rispetto agli altri concorrenti, con circa 5.000 chilometri di cavi rispetto a TE SubCom, leader con quasi 80.000 chilometri negli ultimi cinque anni.

Il problema più rilevante è quello della sorveglianza e dello spionaggio, sia sul luogo di messa in posa sia sulla giunzione dei cavi[37]. Ad oggi, i contenuti sensibili che viaggiano lungo i cavi sono per lo più protetti dalla crittografia tuttavia anche il solo accesso ai metadati può fornire informazioni potenzialmente appetibili[38]. I sistemi di gestione delle infrastrutture di rete sottomarine assicurano infatti un controllo centralizzato che crea notevoli rischi per la sicurezza e può costituire un obiettivo di pirati informatici e paesi ostili[39].

In ogni caso, emerge più in generale la necessità di intensificare la sorveglianza, rafforzare la cooperazione internazionale e alzare la soglia di attenzione, ad ogni livello, su quella che può essere definita una nuova, delicata frontiera della sicurezza globale. L'importanza di assicurare protezione ai cavi sottomarini non è infatti soltanto questione di difesa nazionale e tutela degli interessi strategici ma riguarda anche il corretto funzionamento di internet, l'integrità dei dati e la regolarità delle comunicazioni.

1.3.6. I porti europei nel mirino

L'istituto olandese Clingendael ha pubblicato nel dicembre 2019 fa un rapporto del ricercatore Frans-Paul van der Putten dedicato a "*I porti europei e l'influenza strategica cinese*" (dicembre 2019) che contiene un'analisi accurata delle implicazioni politiche degli investimenti commerciali cinesi nei porti europei fra il 2013 e il 2018.

Il rapporto dimostra come la dipendenza economica di un paese condizioni le sue scelte politiche; al riguardo la Grecia rappresenta il laboratorio in cui tutto ciò è stato sperimentato. Il rilevante peso economico acquisito dalla Cina in quel paese si è tradotto in una estesa e pervasiva influenza di carattere politico che riveste anche connotati strategici.

La lezione che si può trarre è che la questione non è mai solo economica o tecnica.

La Cina ha fatto della componente marittima (MSR, *Maritime Silk Road*) della sua "*Belt and*

[36] J. Smyth, "*Huawei's undersea cable project raises red flag in Australia*," *Financial Times,* dicembre 2017.

[37] T. Davenport, "*Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*", Catholic University Journal of Law and Technology, 2015.

[38] P. Swire, "*Online Privacy and ISPs*" *Institute for Information Security & Privacy at Georgia Tech,* febbraio 2016; K. Bressie, "*Government Surveillance, Hacking, and Network Security: What Can Submarine Cable Operators and Their Customers Do*?" *Emerging Subsea Networks,* 2016.

[39] M. Sechrist, "*New Threats, Old Technology: Vulnerabilities in Undersea Communications in Undersea Communications Cable Network Management System*" *Belfer Center for Science and International Affairs Harvard Kennedy School,* 2012.

Road Initiative" (BRI) il tassello fondamentale di una strategia espansionistica che punta alle infrastrutture di trasporto, energia e comunicazione soprattutto dei paesi in via di sviluppo e di quelli dell'Europa centro-orientale. Avviata su impulso del governo centrale, riguarda settori come le costruzioni navali e il loro finanziamento, la navigazione marittima, la logistica, la costruzione e la gestione di infrastrutture portuali, fino alla pesca e alla costruzione di rompighiaccio. Lo testimonia una presenza crescente in vari porti europei quali per esempio Trieste, Genova, Rotterdam, Valencia, Bilbao, Zeebrugge.

Una delle principali impresi cinesi attive in Europa, insieme a China Merchants Group, CK Hutchison Holdings. Shanghai International Port Group (SIPG). è COSCO Shipping, che dal 2016 controlla il porto greco del Pireo in quanto gestisce due dei tre terminal tramite la sua controllata *Piraeus Container Terminal* (PCT) e ha il controllo operativo del terzo attraverso la quota di maggioranza dell'autorità portuale (PPA).

Si tratta della più grande compagnia di navigazione globale del mondo, terzo maggiore vettore di container e quinto operatore di terminal. Fondata nel 1961 dal governo cinese come impresa statale per la navigazione d'oltremare, le sue attività si sono diversificate fino a comprendere il settore immobiliare e la gestione alberghiera, con l'obiettivo di diventare impresa leader per servizi integrati di logistica e approvvigionamento. Secondo il rapporto Clingendael sono il partito comunista cinese (PCC) e la Commissione statale per la supervisione e l'amministrazione delle attività del Consiglio di Stato (SASAC) ad esercitare sulla società un'influenza rilevante, dati i suoi interessi convergenti con quelli del partito e del governo.

In un recente rapporto i *think tanks* tedeschi GPPi e MERICS hanno evidenziato la stretta correlazione fra gli investimenti di COSCO nel porto del Pireo e l'influenza cinese sulla Grecia. Nel 2016 il governo greco, in piena crisi finanziaria, è stato costretto a ripagare il proprio debito con il Fondo monetario internazionale e l'UE vendendo dapprima la sua quota di maggioranza nella PPA, l'autorità portuale del Pireo (che ha assunto forma societaria nel 1999 ed è stata poi quotata alla borsa di Atene nel 2003) per poi trasferire il 51% delle quote a COSCO per 280,5 milioni di euro. Peraltro, lo strumento principale della leva politica cinese sullo Stato ellenico non è tanto il controllo del porto del Pireo da parte di COSCO quanto la capacità di questa società di indirizzare il traffico di container verso la Grecia.

Occorre ricordare che mentre l'Europa imponeva pesanti restrizioni e sacrifici alla Grecia, i cinesi si facevano avanti con cospicui investimenti, diventando un importante punto di riferimento economico e politico. Si possono forse leggere in quest'ottica le obiezioni di Atene nel 2016 a una presa di posizione critica verso la Cina in risposta a una decisione arbitrale sul Mar Cinese Meridionale, così come nel 2017 il suo veto ad una proposta di risoluzione UE nei confronti della Cina in materia di diritti umani al Consiglio delle Nazioni Unite e, nello stesso anno, la sua opposizione ad un meccanismo di controllo UE degli

investimenti stranieri che, ciononostante, nel 2019 avrebbe visto la luce sotto forma di regolamento (2019/452).

A ciò si aggiunga che la Grecia ha da poco aderito alla cosiddetta piattaforma 16+1 per l'interazione diplomatica ed economica tra Cina e paesi dell'Europa centro-orientale, considerata dalla Commissione europea come una minaccia, un cuneo inserito all'interno dell'UE per minare l'unità dei suoi membri. L'adesione della Grecia si ritiene collegata agli investimenti di COSCO nel Pireo. Tale piattaforma, costituitasi nel 2012 e formalmente conosciuta come Cina–PECO, comprende 16 nazioni dell'Europa centro-orientale di cui 11 sono membri dell'UE e fa da supporto alle iniziative della BRI in Europa, avendo trovato terreno fertile in paesi che sempre più si rivolgono a Pechino come principale finanziatore di infrastrutture fisiche e digitali.

Come una sorta di UE in scala ridotta, prevede il coordinamento di una serie di attività in settori che vanno dalla normativa ambientale ai collegamenti aerei e comprende alcune collaborazioni scientifiche[40]. La Lituania, per esempio, coordina la cooperazione nel settore agricolo compresa la ricerca, mentre la Romania ospita un centro di ricerca e sviluppo. Vari centri di medicina tradizionale cinese (MTC) operano in università ungheresi, montenegrine e della Repubblica Ceca, in stretto contatto con università cinesi e la *China Academy of Chinese Medical Sciences* per diffondere tali pratiche in tutta Europa.

Come rileva Bart Broer, ricercatore presso il Centro UE-Asia di Bruxelles, a differenza di quelli europei, i prestiti cinesi non sono condizionati al rispetto dei diritti umani, dello stato di diritto e dei valori democratici da parte dei paesi destinatari. I leaders delle nazioni dell'Europa centrale e orientale hanno accolto con favore il sostegno finanziario cinese con l'obiettivo di accelerare lo sviluppo economico del proprio paese. E' peraltro significativo che in tali paesi sia del tutto assente una riflessione sui potenziali rischi degli investimenti cinesi nel 5G e più in generale nel settore delle tecnologie, a differenza di quello che sta avvenendo Germania, Francia o Regno Unito, per esempio.

Il timore – come rileva Broer - è che Pechino si serva della piattaforma 16+1 non solo per perseguire obiettivi commerciali, ma sfrutti i suoi investimenti e prestiti per acquisire risorse strategiche e accumulare influenza politica, cercando di dividere il fronte europeo che solo di recente ha preso consapevolezza della delicatezza e delle insidie insite negli investimenti cinesi in particolare nelle infrastrutture critiche. Si può ritenere che ciò sia avvenuto solo nel marzo 2019, con l'adozione del regolamento 2019/452 sul controllo degli investimenti stranieri (a cui è dedicato il par. 3.5), con cui gli Stati membri sono invitati a valutare i potenziali effetti sulla sicurezza e l'ordine pubblico degli investimenti diretti esteri in infrastrutture critiche e tecnologie avanzate, ivi compresi i porti marittimi.

Dopo la Grecia, potrebbe essere il turno del Montenegro, paese dei Balcani occidentali in procinto di aderire all'UE, che nel 2014 ha concluso un accordo

[40] Così A. ROUSSI in "A path to Europe", Nature, 9 maggio 2019.

con Exim Bank, banca per l'import-export di proprietà statale cinese, per finanziare l'85% di un progetto di costruzione di un'autostrada di 165 chilometri, per una somma pari a un quarto del prodotto interno lordo del paese. I costi dell'autostrada hanno fatto aumentare in modo considerevole il debito pubblico del Montenegro che - secondo Broer – qualora non sia redditizia, non sarà in grado di ripagare il proprio debito e quindi costretto ad affidarne la gestione e probabilmente la stessa proprietà alla banca.

Anche in questo caso varrebbe la pena rammentare il "*timeo danaos et dona ferentes*": ogni cosa ha un prezzo e il conto da pagare rischia di essere piuttosto caro, come l'esperienza greca insegna. Una lezione per l'intera Europa, Italia compresa.

2. MINACCIA *CYBER E* SICUREZZA NAZIONALE

2.1. Lo spazio cibernetico

L'accresciuta dipendenza della nostra società dai dati e dalle reti di comunicazione, pubbliche o private, è tale da rendere molto rilevanti i danni che potrebbero derivare da attacchi mirati, che normalmente hanno come bersaglio i soggetti più fragili e i sistemi meno protetti. Si tratta di fattispecie che possono essere molto diverse fra loro, presentare distinte caratteristiche ed essere qualificabili come crimini di varia natura, dalla realizzazione di furti e truffe allo scambio *on-line* di materiale pedopornografico, dalla compromissione della difesa militare di un Paese al danno economico arrecato agli interessi di società o privati individui.

Questo scenario rende necessario, per le istituzioni ed i cittadini, disporre di una cornice normativa adeguata[41], atta a garantire sicurezza al cosiddetto spazio cibernetico, alla cui definizione concorrano al tempo stesso entità pubbliche e soggetti privati, *in primis* i proprietari e gestori degli *asset* critici, la cui integrità e tutela devono essere assicurate in modo efficace.

Lo spazio cibernetico viene definito come l'insieme delle infrastrutture informatiche interconnesse, ivi inclusi *hardware*, *software*, dati ed utenti, nonché le relazioni logiche, comunque stabilite, tra di essi. Pertanto comprende internet, le reti di comunicazione, i sistemi in cui operano i processi informatici di elaborazione dati e gli apparati mobili dotati di connessione di Rete. In tal senso una minaccia cibernetica può essere costituita da tutte quelle condotte suscettibili di svolgersi nello spazio cibernetico oppure in danno di esso e può assumere varie forme e connotazioni. Ne sono esempio le azioni aggressive nei confronti di un *network* o una parte delle sue componenti da parte di singoli individui o entità, statuali o meno, miranti a eliminare, danneggiare o compromettere il regolare funzionamento

[41] In generale, sugli sviluppi della disciplina della cybersicurezza, si vedano H. CARRAPICO – A. BARRINHA, *The EU as a coherent (cyber) security actor?*, in *JCMS: Journal of Common Market Studies*, 2017; J. RUOHONEN – S. HYRYNSALMI – V. LEPPÄNEN, *An outlook on the institutional evolution of the European Union cyber security apparatus*, in *Government Information Quarterly* 33.4, 2016, 746-756; R. H. WEBER – E. STUDER, *Cybersecurity in the Internet of Things: Legal aspects*, in *Computer Law & Security Review* 32.5, 2016, 715-728.

dei sistemi e delle reti, oppure a incidere sull'integrità, la disponibilità e la riservatezza dei dati ivi custoditi o trasmessi. Alcuni attacchi possono assumere caratteri particolarmente sofisticati e svolgersi tramite l'uso di cosiddette "armi cibernetiche", quali *software* malevoli appositamente sviluppati ("*malware*")[42], o una serie di istruzioni informatiche miranti a distruggere o alterare un sistema. Si tratta di minacce particolarmente insidiose in quanto spesso di difficile individuazione che si esplicano attraverso modalità cosiddette asimmetriche[43].

Per delineare la natura della minaccia, è utile distinguere tra varie tipologie in base alle finalità perseguite. Pertanto si fa riferimento a:

- criminalità cibernetica (*cyber-crime*): insieme delle attività aventi obiettivi criminali (la truffa o la frode telematica, il furto d'identità, la sottrazione indebita o l'alterazione di informazioni o la violazione dei diritti di proprietà intellettuale)[44]. In ambito europeo la definizione, molto generale, che ne fornisce la Commissione europea in una comunicazione del 2007, comprende "*gli atti criminali commessi contro reti di comunicazioni elettroniche e sistemi di informazione o avvalendosi di tali reti e sistemi*"[45].

- spionaggio cibernetico (*cyber-espionage*), consistente nell'acquisizione indebita di dati/informazioni sensibili, proprietarie o classificate;

- terrorismo cibernetico (*cyber-terrorism*), che consta dell'insieme delle azioni ideologicamente motivate, miranti a condizionare uno Stato o un'organizzazione internazionale[46];

---

[42] Il *malware* è un *software* deleterio creato per danneggiare computer collegati ad una Rete, sfruttando la loro vulnerabilità e inducendoli così ad azioni diverse da quelle a cui sono dedicati. G. TAPPERO MERLO, *Il dominio degli spazi: il cosmo, la cyberwar e l'urgenza di una dottrina operativa per la guerra futura,* in *La Comunità Internazionale,* Fasc. 4/2010, 535-559.

[43] L'"asimmetria" consiste nel fatto che colui il quale pone in essere tali minacce può colpire a grandissima distanza, da ovunque esista un accesso alla Rete. Potenzialmente può attaccare sistemi particolarmente sofisticati e protetti sfruttandone anche una sola vulnerabilità, può agire con tempi tali da non consentire un'efficace reazione difensiva, può rimanere anonimo o comunque non facilmente individuabile rendendo in tal modo estremamente complessa e difficile una risposta da parte dell'attaccato. Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013, 11.

[44] S. BRENNER, *Defining cyber-crime: A review of federal and state law,* in R.D. CLIFFORD (Ed.), *Cybercrime*, Carolina Academic Press, 2001, 15-104, 17; L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec*., 4, 2011, 827 ss.

[45] Commissione europea, *Verso una politica generale di lotta contro la* cyber-criminalità*,* COM(2007)267, Bruxelles. Un importante riferimento in materia è anche la Convenzione del Consiglio d'Europa sulla *cyber*-criminalità del 2001.

[46]Consiglio dell'Unione europea, *Statement on tighter International security*, 16751/08, 2008, Bruxell es. Si veda, al riguardo, *Guerra preventiva*, in A. CIPRIANI - G. CIPRIANI, *La nuova guerra mondiale. Terrorismo e intelligence nei conflitti globali,* Milano, 2005, 27-36. È stato attribuito a Osama Bin Laden anche il primato di aver lanciato il primo manifesto sul *cyber*-terrorismo, nel 2000, dal titolo *Al-jihad al-electronic.* Si veda F. GHIONI, *Hacker Republic*, Milano, 2009, 61; E. ALSHECH, *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*, The Jerusalem Post, 28 febbraio 2007.

- guerra cibernetica (*cyber-warfare*), cioè l'insieme delle attività e delle operazioni militari pianificate e condotte allo scopo di conseguire effetti nel destinatario[47]. Si pensi all'utilizzo nel 2010 del *malware* Stuxnet[48] per attaccare alcuni impianti iraniani di arricchimento dell'uranio[49], che ha segnato un punto di svolta decisivo nel dibattito circa la possibilità, fino ad allora meramente teorica, di danneggiare fisicamente l'infrastruttura critica di una nazione sfruttando i sistemi informatici che la governano. Il tema del *cyber-warfare* è solo vagamente affrontato nei documenti strategici dell'UE[50], essendo considerato di esclusiva competenza della NATO oltre che degli Stati membri. E' tale organizzazione ad aver promosso un ampio dibattito sull'opportunità di far fronte alla possibilità di attacchi cibernetici su larga scala, come quelli perpetrati ai danni dell'Estonia nel 2007[51] e della Georgia nel 2008[52] quali fattispecie rientranti negli artt. 4 e 5 del Trattato di Washington (l'atto istitutivo della NATO), tali dunque da attivare la clausola di difesa collettiva tra gli alleati[53].

Come rilevato, un elemento caratteristico del crimine perpetrato nello spazio cibernetico consiste nel profondo *vulnus* economico che esso produce[54]. Sulla rete internet, per esempio, sono trasmesse e immagazzinate quantità crescenti di dati aziendali o concernenti lo *status* patrimoniale degli individui (in particolare grazie ai servizi di *cloud computing)*, nonché dati afferenti a delicate transazioni e attività finanziarie, economiche e commerciali. Questa situazione rende gli attacchi

[47] Si veda J. ARQUILLA - D. RONFELDT, *Cyberwar is Coming!,* in *Comparative Strategy*, Vol. 12, No. 2, Spring 1993, 141-165.

[48] I. R. PORCHE - J. M. SOLLINGER - S. MCKAY, *A Cyberworm that Knows no Boundaries*, Rand Occasional Paper, Santa Monica (Ca), 2011. Per un'analisi completa ed esaustiva degli aspetti tecnici del malware Stuxnet, tra gli altri, M. DE FALCO, *Stuxnet Facts Report - A Technical and Strategic Analysis*, NATO CCD COE Publications, 2012.

[49] P. WOODWARD, *Iran confirms Stuxnet found at Bushehr nuclear power plant*, 2010; Foreign Policy, *6 mysteries about Stuxnet*, 2010, in http://blog.foreignpolicy.com/posts/2010/09/27/6_mysteries_about_stuxnet.

[50] Consiglio dell'Unione europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza, Garantire sicurezza in un mondo in piena evoluzione*, 2008.

[51] N. SHACHTMAN, Estonia, *Google Help 'Cyberlocked' Georgia*, in *Wired*, 11 agosto 2008.

[52] Si veda S. W. KORN – J. E. KASTENBERG*, Georgia's Cyber Left Hook*, in *Parameters*, Winter 2008-09, 60-76.

[53] La politica di cyberdifesa è attuata dalle autorità politiche, militari e tecniche della NATO cosi come dai singoli Stati alleati. Uno dei principali aspetti di questa politica è stata la creazione della NATO *Cyber Defence Management Authority* (CDMA), con la responsabilità di coordinare la difesa informatica in tutti i quartieri generali dell'Alleanza dei comandi e nelle agenzie associate spostando le molteplici reti informatiche di oggi verso un sistema amministrato a livello centrale. Il CDMA della NATO è gestito dal *Cyber Defence Management Board*, che comprende i responsabili degli uffici politici, militari, operativi e tecnici della NATO che si occupano di difesa informatica. Il CDMA è il principale organo di consulenza del Consiglio Atlantico in materia di difesa informatica e offre pure consulenza agli Stati membri su tutti i principali aspetti della difesa cibernetica. Il CDMA della NATO opera sotto l'egida della divisione *Emerging Security Challenges* (sfide emergenti alla sicurezza) del NATO HQ (comando e staff). NATO, *Defending against cyber attacks*, http://www.nato.int/cps/en/natolive/ topics_49193.htm.

[54] S. BLITZBLAU, *Cyber-Espionage Threats and Impacts on Italian Economy and Businesses*, Maglan Europe srl, relazione presentata alla 2° International Warfare Conference, Roma, 27 ottobre 2011.

cibernetici potenzialmente assai lucrativi, esponendo a grave rischio le imprese, gli istituti bancari e finanziari, gli enti governativi preposti al controllo dell'attività economica e produttiva nazionale, in quanto terminali di informazioni strutturate digitalmente e contenenti dati personali, industriali, finanziari e gestionali. Le informazioni trasmesse *on-line* (i dati) sono state assimilate, per importanza e valenza strategica, alle materie prime essenziali per il funzionamento di una nazione e il suo successo nell'arena internazionale come il petrolio, il gas o i metalli rari[55].

Gli attacchi *cyber* minano quella che è stata definita come *business continuity,* avvantaggiandosi di diversi tipi di vulnerabilità del sistema, siano esse organizzative o tecniche. Le debolezze del *network* possono derivare dalla mancata attuazione delle misure preposte alla protezione da *malware,* tramite *best-practices* e strumenti *anti-virus* e *anti-spam* adeguati, tuttavia possono anche essere frutto dell'assenza o dell'insufficiente attuazione di meccanismi di sicurezza fisica che siano in grado di assicurare un livello minimo di continuità del servizio e ridimensionare le conseguenze negative di eventi, anche naturali, che arrecano danni all'infrastruttura del *networ*k[56]; di qui la necessità di approntare con tempestività una serie di misure adeguate ed efficaci. Le vulnerabilità strettamente tecniche sono invece quelle generalmente riconducibili a lacune nei sistemi di sicurezza del *software* applicativo e dei protocolli di comunicazione adottati[57].

Il governo italiano ha da tempo concentrato la propria attenzione sul tema della sicurezza nello spazio cibernetico. Nel 2010 la Relazione sulla politica dell'informazione per la sicurezza evidenziava che, "*con riferimento agli scenari di potenziale incidenza sulla sicurezza economica e sulla più generale architettura di sistema che sorregge il concreto funzionamento, le attività quotidiane e i programmi di sviluppo della Nazione, un fondamentale campo di sfida per l'intelligence sarà quello della cybersecurity. Ciò a cospetto di una minaccia che ha ormai assunto caratura strategica, tanto da essere considerata dai principali attori internazionali un fattore di rischio di prima grandezza, direttamente proporzionale al grado di*

[55] F. VITALI, *L'oro nero dei dati*, in Limes, n. 7, luglio 2014, 29; G. TAPPERO MERLO, *Soggetti e ambiti della minaccia cibernetica: dal sistema paese alle proposte di cyber governance*? in *La Comunità Internazionale*, Fasc. 1/2012, 25-53. L'autore sottolinea: «*Così come per questi elementi si è giunti, negli ultimi decenni, anche a scontri per il loro accaparramento e il loro controllo, così per la tutela di quell'insieme di dati che compongono la ricchezza delle nazioni più industrializzate è necessario operare a livello globale. Si tratta di un complesso di informazioni su progetti, brevetti, piani strategici e quant'altro messo in una Rete che, anche se garantita da muri digitali di protezione è, a quanto sembra, ancora troppo vulnerabile. Infatti, a rischiare attacchi cibernetici sono proprio i paesi a maggior dotazione di know how innovativo e con alta esposizione in Rete. È la doppia faccia di internet e dei vantaggi che offre l'innovazione dei sistemi ICT* […]».

[56] Si veda 2016 *Italian Cybersecurity Report*. Controlli Essenziali di Cybersecurity, (a cura di) R. BALDONI – L. MONTANARI – L. QUERZONI, Cis Sapienza, marzo 2017. Laboratorio Nazionale CINI di Cybersecurity - Consorzio Interuniversitario Nazionale per l'Informatica, Versione 1.0, marzo 2017.

[57] Si considerino per esempio quelle che concernono il *Domain Name System* (DNS), il cui sfruttamento «*può avere ripercussioni sia sugli utenti che usufruiscono dei servizi di comunicazione elettronica sia sui gestori di infrastrutture critiche informatizzate*» in Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico,* dicembre 2013, 16.

sviluppo raggiunto dalle tecnologie dell'informazione"[58]. Gli obiettivi delineati erano quelli di potenziare le capacità di difesa delle infrastrutture critiche nazionali, incentivare la cooperazione tra istituzioni ed imprese nazionali, promuovere la cultura della sicurezza cibernetica, rafforzare la cooperazione internazionale.

Il crimine informatico viene infatti ritenuto "*una piaga che può decretare il fallimento delle aziende, la sottrazione del loro patrimonio tecnologico e che depaupera la ricchezza delle nazioni*", e la sua rilevanza negativa appare evidente, in quanto "*sfrutta la vulnerabilità dei sistemi informatici per sottrarre il frutto del nostro lavoro di ricerca e sviluppo nel campo delle nuove tecnologie e dei prodotti. Per un Paese come l'Italia, che fa dell'innovazione la pietra angolare della sua crescita e della sua competitività, il danno potenziale è incalcolabile*".

Il tema della sicurezza cibernetica acquisisce ulteriore rilevanza nelle successive relazioni presentate dal governo al Parlamento, in cui la minaccia cibernetica viene qualificata come suscettibile di avere "*un potenziale impatto sul sistema Paese e sulla stessa sicurezza nazionale*"[59], diventa meritevole di una "*prioritaria attenzione*"[60] e considerata alla stregua della "*sfida più impegnativa per il sistema Paese*"[61].

2.2. Sicurezza e libertà. La centralità del dato nel capitalismo delle piattaforme digitali

Risulta pertanto essenziale elaborare un adeguato sistema di prevenzione, informato ai principi dell'analisi del rischio, della gestione e mitigazione del medesimo in modo tale da garantire la sicurezza fisica, logica e procedurale dello spazio cibernetico. Si tratta in pratica della cosiddetta cybersicurezza*,* individuata dall'*International Telecommunication Union* (ITU) delle Nazioni Unite, nell'*"insieme di strumenti, interventi, concetti, linee guida, impostazioni della gestione del rischio, azioni, pratiche, procedure e tecnologie che possono essere utilizzate per proteggere lo spazio e la struttura cibernetici e i loro utilizzatori*"[62].

La cybersicurezza[63] è definibile come "*l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"* (in questi termini si esprime il regolamento UE 2019/881, il c.d. *Cybersecurity Act*).

La cybersicurezza rappresenta dunque il contesto in cui si elaborano le regole che disciplinano le interrelazioni tra i diversi soggetti che operano nello spazio cibernetico. Ha dunque uno spiccato carattere sovranazionale e dematerializzato; è l'arena ove si misura quell'insieme di informazioni che la tecnologia permette di raccogliere, elaborare, diffondere e immagazzinare, attraverso la Rete. In questo

[58] Governo italiano, *Relazione sulla politica dell'informazione per la sicurezza 2009*, 2010, 93.
[59] Governo italiano, *Relazione sulla politica dell'informazione per la sicurezza 2010*, 2011, 30-32.
[60] Governo italiano, *Relazione sulla politica dell'informazione per la sicurezza 2011*, 2012, 65-70.
[61] Governo italiano, *Relazione sulla politica dell'informazione per la sicurezza 2012*, 2013, 37-47.
[62] UN ITU, *Overview of Cybersecurity. Recommendation* ITU-T X.1205, Geneva, United Nations, aprile 2008.
[63] Cfr MENSI M. e FALLETTA P.*, Il diritto del web,* Padova, 2018, capitolo XI*,*

senso, la cybersicurezza costituisce un essenziale strumento globale di garanzia e di difesa anche della conoscenza e della libertà di espressione[64] che mediante internet è veicolata, ed è pertanto giustificato che sia destinataria di adeguati investimenti, in termini di risorse tecniche, economiche e cognitive[65].

Ai rischi connessi alla vulnerabilità dei sistemi informatici non sfuggono neppure i meccanismi di formazione del consenso elettorale, come emerge per esempio dalla decisione assunta dal Presidente degli Stati Uniti, nel dicembre 2016, di espellere funzionari diplomatici russi in risposta agli attacchi *hacker* subiti dal partito democratico durante la campagna elettorale del novembre 2016[66]. L'*intelligence* statunitense ha infatti evidenziato come *hacker* russi, attraverso l'uso di *software* e *malware* sofisticati, avessero illegalmente ottenuto accesso ai server del partito democratico e sottratto informazioni riservate per poi diffonderle sui mezzi di comunicazione elettronica, in modo da influenzare, seppur di riflesso, il risultato delle elezioni presidenziali[67]. Ecco perché l'esigenza di dotarsi di strumenti sempre più efficaci per contrastare la criminalità cibernetica è ormai diffusa tra i governi di tutto il mondo.

Gli Stati hanno pertanto ricalibrato le proprie infrastrutture tecnologiche al fine di includere funzionalità di intercettazione (*backdoors*) per consentire una maggiore sorveglianza, rendendo le reti telefoniche moderne accessibili da remoto e controllabili. E' aumentata la quantità di dati riguardanti gli individui (i cosiddetti "metadati") contenenti informazioni personali sulle attività *on-line e off-line* che

[64] Si veda O. A. HATHAWAY e altri, *The Law of Cyber-Attack*, *Yale Law School*, novembre 2011; G. TAPPERO MERLO, *supra* nota 15.

[65] Si veda N. VAN DER MEULEN - E. A JO – S. SOESANTO , *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses,* studio commissionato dal Parlamento europeo, 18 novembre 2015, che contiene un'ampia disamina delle capacità cyber sulla base di tre direttrici principali: *cyberresilience, cybercrime* e *cyberdefence*.

[66] Si veda L. GAMBINO – S. SIDDIQUI – S. WALKER*, Obama expels 35 Russian diplomats in retaliation for US election hacking*, The Guardian, 30 dicembre 2016.

[67] Sebbene ricostruire la dinamica di un attacco informatico e ricondurlo ad una fonte certa sia un'operazione molto articolata, occorre rilevare che a sostegno della tesi che riconosce la Russia quale mandante dell'attacco vi sono anche le risultanze dell'indagine interna aperta dal partito democratico ed affidata ad un'azienda specializzata in sicurezza informatica, che sembrerebbe aver ricondotto la sottrazione dei dati riservati e la successiva pubblicazione *online* degli stessi a due diversi *hacker,* soprannominati "Cozy Bear" e "Fancy Bear", asseritamente legati ai servizi e all'intelligence militare russa. Si veda, S. THIELMAN – S. ACKERMAN *Cozy Bear and Fancy Bear: did Russians hack Democratic party and if so, why?*, The Guardian, 29 luglio 2016. Per un'analisi della vicenda, S. KREPS – D. DAS, *Warring from the virtual to the real: Assessing the public's threshold for war over cyber security*, in *Research & Politics* 4.2, 2017; D. P. FIDLER, *The US Election Hacks, Cybersecurity, and International Law*, in *American Journal of International Law* 110, 2016: 337-342. In ambito nazionale, il tema dello spionaggio cibernetico si è imposto all'attenzione dell'opinione pubblica in seguito alla vicenda che ha portato all'arresto dei fratelli Giulio e Francesca Maria Occhionero, con l'accusa di aver violato gli account email di numerosi personaggi, in specie politici, attraverso l'uso di *malware*. Sulla vicenda, J. SNOW, *EyePyramid, Malware spensierato,* 13 gennaio 2017, https://www.kaspersky.it/blog/eye-pyramid-spyware/9579/

sono automaticamente immagazzinate dagli operatori[68] e la cui analisi, all'esito di combinazioni e aggregazioni operate attraverso l'applicazione di algoritmi sofisticati, può risultare estremamente invasiva[69]. Questo è stato evidentemente favorito dalla proliferazione e affinamento delle tecnologie di intercettazione, monitoraggio e analisi delle comunicazioni, a costi vieppiù decrescenti (per esempio attraverso il *targeting* comportamentale[70], realizzato mediante "*cookie*"[71], "*super-cookie*", "*device fingerprinting*", "*deep packet inspection*").

La natura dinamica della tecnologia non solo ha cambiato il modo in cui la sorveglianza può essere effettuata, ma anche "cosa" può essere monitorato. Questa "tentazione tecnologica" orientata al controllo globale può talora apparire irresistibile anche per gli Stati democratici[72]. D'altronde il *web* risulta oggi il

[68] *WhatsApp* all'atto dell'installazione acquisisce la rubrica dell'utente (secondo i *Terms of service*) ed è libera di trasformare (si parla di *datizzazione*) in metadati economicamente valorizzabili i rapporti inter-personali/inter-aziendali ed i collegamenti da essa risultanti. Il valore della società è legato al valore intrinseco dei Big Data riferiti ad oltre 400 milioni di utenti attivi ogni mese.

[69] Secondo i risultati di una ricerca della società IDC, alla fine del 2020 ci sarà una quantità di "*digital data*" 44 volte maggiore rispetto al 2009, e l'ammontare dei dati raddoppia ogni 20 mesi.

[70] Gran parte della raccolta di dati personali su internet è legata al *targeting* comportamentale, nonostante studi indichino che la maggior parte dei cittadini interpellati non intendono ricevere pubblicità comportamentale mirata. Il *targeting* comportamentale consiste nel monitoraggio del comportamento *on-line* degli utenti al fine di utilizzare le informazioni raccolte per indirizzare gli individui tramite pubblicità che siano corrispondenti ai loro interessi precedentemente individuati e ad esso si applicano le norme europee in tema di protezione dei dati. Il regolamento 2016/679 definisce i "dati personali" come "qualsiasi informazione concernente una persona fisica identificata o identificabile" ("*data subject*") (art. 4, n. 1) e tale definizione include gli "identificatori *on-line*". La Corte di giustizia dell'Unione europea, così come le autorità europee, ha rilevato che anche le informazioni senza nome possono essere considerate "dati personali", in quanto consentono di distinguere una persona all'interno di un gruppo (così come i *cookies* utilizzati per il *targeting* comportamentale).

[71] Si distinguono diverse categorie di *cookie* a seconda delle loro caratteristiche tecniche e funzioni: a) *HTML cookie*, per lo più incorporati nelle informazioni HTML (per esempio, le pagine web viste) che il computer ed il *server* si trasmettono per consentire la personalizzazione delle informazioni utili alla navigazione degli utenti. b) *Flash cookie*, associati al software Adobe Flash. C) *Web bug, Web beacon, tracking bug, pixel tag, cookie anchor*, ecc. (la tipologia più utilizzata per il tracciamento), che possono essere inclusi in una pagina *web* o in una email e consentono di verificare non solo le pagine viste, ma anche le azioni compiute dall'utente (parole digitate, ricerche effettuate, annunci pubblicitari selezionati, frasi evidenziate, preferenze di acquisto e anche i mezzi di pagamento utilizzati, movimenti del mouse), nonché le informazioni di dettaglio (come l'indirizzo IP).

[72] Interessanti al riguardo le considerazioni di E. Morozov, intellettuale bielorusso che vive negli Stati Uniti, esperto di nuove tecnologie, che descrive i tempi attuali nei termini di un'"apocalisse informativa", in cui i dati personali sono merce sempre più accessibile: "Il vecchio e radicato mito secondo cui esiste uno spazio virtuale autonomo dove è possibile avere più *privacy* e indipendenza dalle istituzioni sociali e politiche è morto. […] Cosa succederà fra cinque anni, quando tutti gli oggetti e i dispositivi diventeranno smart, cioè avranno dei sensori avanzati e poco costosi, e saranno collegati tra loro e con internet? […] tutti questi oggetti lasciano delle tracce di dati. […] Seguendo un modello […] già oggi disponibile grazie a diverse *startup* note come *personal data lockers*, archivi personali di dati, possiamo fare soldi vendendo noi stessi i nostri dati […] Sostanzialmente, la possibilità di inserire un sensore e un collegamento internet in qualunque cosa, compreso il corpo umano, consente di mercificare tutto e di attribuire un prezzo alle informazioni che se ne ricavano. I sensori e la connettività permanente contribuiscono a creare nuovi mercati nel campo

contesto più propizio per l'esercizio da parte delle autorità pubbliche (e, sovente, private), direttamente o indirettamente, di un monitoraggio generalizzato, che trova per lo più la sua giustificazione nella tutela dell'ordine pubblico e nella protezione della sicurezza nazionale dai pericoli derivanti dal terrorismo[73].

Talora ci si trova di fronte alla realtà di un utilizzo non regolato di informazioni suscettibile di incidere profondamente sui diritti fondamentali alla *privacy* e alla protezione dei dati personali, sanciti dalla Carta dei diritti fondamentali dell'Unione europea del 2009, la cui disciplina di dettaglio è contenuta per lo più nel regolamento UE 2016/679.

Risulta pertanto essenziale trovare un equilibrio tra la tutela della sicurezza nazionale e il rispetto dei diritti di libertà, *in primis* della *privacy* dei cittadini[74]*,* fermo restando la legittimità l'intervento dell'autorità pubblica in presenza di rischi per la sicurezza nazionale, laddove questo sia necessario e proporzionale all'obiettivo perseguito[75].

Al riguardo giova ricordare che il concetto di "sicurezza nazionale" appare per lo più indefinito nelle varie normative nazionali, talora ancorato a parametri tanto vaghi e indeterminati da rendere accettabile e giustificato ogni intervento di intercettazione e accesso alle comunicazioni personali[76].

Al riguardo de Vergottini[77] indica che la nostra costituzione considera la sicurezza come valore essenziale riservato alla competenza dello Stato. Spetta infatti allo

---

dell'informazione, permettendo ai cittadini di monetizzare l'autosorveglianza. […] Per gran parte degli anni novanta, tutti hanno creduto che la digitalizzazione avrebbe aperto la strada alla cosiddetta "convergenza", sicuramente un'ottima cosa per quanto riguarda la sicurezza. Il ragionamento era questo: passando a un'unica Rete, le precedenti forme di comunicazione (il caro vecchio telefono e simili) diventeranno sicure come la posta elettronica cifrata. In realtà siamo andati nella direzione opposta. Quello che abbiamo oggi è sì un'unica Rete, ma la sicurezza e le privacy sono tornate al livello della rete telefonica. E' il telefono, non la posta elettronica, il nostro comune denominatore per quanto riguarda la sicurezza, almeno in termini di capacità di intercettazione. La convergenza c'è stata ma, miracolosamente, le tecnologie sono riuscite a convergere sull'opzione meno sicura e più facile da sorvegliare", E. MOROZOV, *Il mercato dei dati, Frankfurter Allgemeine Zeitung,* in *Internazionale,* 6 settembre 2013.

[73] S veda F. VITALI, *Comunicazione e controllo ai tempi del terrore*, in Limes – Rivista italiana di geopolitica, n.11, 2015, 141-146.

[74] J. E. COHEN, *What Privacy Is For*, 126 *Harv. L. Rev*. 1904, 1906, 2013.

[75] Quando la pratica delle intercettazioni ebbe inizio negli Stati Uniti d'America, era condotta in base a criteri molto rigidi. Nella prima convalida giudiziaria delle intercettazioni, il giudice Brandeis della Corte Suprema espresse un netto dissenso, rilevando che le intercettazioni costituivano un "*mezzo di vasta portata suscettibile di violare la* privacy" e dunque difficilmente giustificabile ai sensi della Costituzione (1928). Le intercettazioni erano infatti percepite come un mezzo estremamente rischioso per la *privacy,* il cui uso doveva essere limitato e volto a individuare e perseguire i reati più gravi. Nel corso del tempo, tuttavia, gli Stati hanno ampliato i loro poteri di sorveglianza, abbassando la soglia di tutela della *privacy* e aumentando le cause giustificatrici dell'esercizio di tali poteri di monitoraggio.

[76] F. LA RUE, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* United Nations, General Assembly, 17 aprile 2013, par. 58.

[77] G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in Rivista AIC, n. 4/2019, 11/11/2019.

Stato, con esclusione delle autonomie territoriali, la difesa e quindi l'assicurazione della sicurezza nei rapporti internazionali ("*difesa e forze armate; sicurezza dello Stato"*: art. 117, comma 1, lettera d) come pure la sicurezza nei rapporti interni ("*ordine pubblico e sicurezza*", ivi, lettera h), da interpretarsi come la "*tutela dell'ordinata e civile convivenza nella comunità nazionale*" (cfr. Corte Costituzionale, sentenze 226 del 2010, 35 del 2011, 118 del 2013)[78]. "*La sicurezza dello Stato costituisce, infatti, un «interesse essenziale, insopprimibile della collettività, con palese carattere di assoluta preminenza su ogni altro, in quanto tocca* […] *la esistenza stessa dello Stato», del quale la giurisdizione costituisce soltanto «un aspetto»* (sentenze n.40 del 2012, n. 106 del 2009, n. 110 del 1998 e n. 86 del 1977)*"*[79].

A livello normativo sono gli articoli 6 e 7 della legge 124/2007 a definire cosa si intende per sicurezza nazionale: la "*difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica*" oppure la "*sicurezza interna della Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica*", soprattutto attraverso l'insieme dei compiti assegnati allora a SISMI e SISDE (oggi rispettivamente AISE ed AISI). Al riguardo la legge 133/2012 non ha

[78] Con particolare riferimento alla concezione di sicurezza quale esigenza di tutela nei rapporti con terzi stati, De Vergottini indica che la Corte nella sentenza n. 86 del 1977 ha poi precisato che la stessa "*trova espressione, nel nostro testo costituzionale, nella formula solenne dell'art. 52, che afferma essere sacro dovere del cittadino la difesa della Patria. Richiamando e sviluppando tale concetto, che trova fondamento nella individuazione di un interesse costituzionale superiore, occorre fare riferimento proprio al concetto di difesa della Patria ed a quello di sicurezza nazionale (del quale ultimo è cenno nell'art. 126 della Costituzione ed in numerose altre disposizioni degli Statuti delle Regioni ad autonomia speciale). Il primo concetto, quello di difesa della Patria, può avere una accezione molto larga ed abbracciare anche aspetti che vanno al di là di quel che in effetti merita di trovare una protezione che valga a superare* […] *altri principi che pur sono ritenuti essenziali[78]. Ma si può osservare che in altre disposizioni il concetto di difesa assume un significato più specifico, come nell'art. 87 Cost. che prevede un organo ad hoc denominato Consiglio supremo di difesa e che certamente, anche nel silenzio della norma, ha compiti attinenti in maniera rigorosa ai problemi concernenti la difesa militare e, pertanto, la sicurezza dello Stato. E proprio a questo concetto che occorre fare riferimento, ponendo il concetto stesso in relazione con altre norme della stessa Costituzione che fissano elementi e momenti imprescindibili del nostro Stato: in particolare vanno tenuti presenti la indipendenza nazionale, i principi della unità e della indivisibilità dello Stato (art. 5 Cost.) e la norma che riassume i caratteri essenziali dello Stato stesso nella formula di "Repubblica democratica" (art. 1 Cost.)"*. La Corte, in altri termini, ha posto in relazione la suprema finalità di sicurezza dello Stato - comunità (espressione - ex art. 52 Cost. - del sacro dovere di difesa della Patria) con tre peculiari parametri costituzionali, ovvero: a) l'indipendenza nazionale; b) i principi di unità ed indivisibilità dello Stato (art. 5 Cost.); c) la disposizione inerente ai caratteri essenziali dello Stato sotto la formula di "Repubblica democratica" (art. 1 Cost.). Tale ricostruzione è stata confermata dalla sentenza n. 24 del 2014, in cui la Corte ha: "[…] *ribadito che la disciplina del segreto involge il supremo interesse della sicurezza dello Stato - comunità alla propria integrità ed alla propria indipendenza, interesse che trova espressione nell'art. 52 della Costituzione in relazione agli artt. 1 e 5 della medesima Carta"* (si veda A. MITROTTI, *Brevi considerazioni sulla disciplina del segreto di Stato*, in AIC – Osservatorio costituzionale, 2/2018, 5 luglio 2018).

[79] *Ibid.*; cfr. anche, in termini simili, Corte costituzionale, sent. n. 24 del 13-2-2014, *sub* 5 cons. in dir.

cambiato l'impianto di fondo della legge 124/2007.

Un interessante chiarimento concettuale, anche se non di valenza normativa, ci viene offerto dal *Glossario Intelligence* del DIS (giugno 2012) che, alla voce "Sicurezza nazionale" indica, pur segnalando il carattere dinamico del concetto, che "*l'indipendenza, l'integrità e la sovranità della Repubblica, la comunità di cui essa è espressione, le istituzioni democratiche poste dalla Costituzione a suo fondamento, la personalità internazionale dello Stato, le libertà fondamentali ed i diritti dei cittadini costituzionalmente garantiti nonché gl'interessi politici, militari, economici, scientifici ed industriali dell'Italia*".

Al riguardo, significativo l'articolo 1 della legge francese del 15 novembre 2001 n. 1062: "*La sicurezza è un diritto fondamentale. Essa è una condizione per l'esercizio delle libertà e per la riduzione delle diseguaglianze*", oltre che essere definita come dovere di intervento in chiave di garanzia per i cittadini. Tale definizione – prosegue De Vergottini - si allinea alla giurisprudenza del *Conseil Constitutionnel* che ha ricompreso la sicurezza fra i valori costituzionali[80]. Scopo della legge, e in particolare degli interventi della magistratura, è quindi "*fissare un equilibrio fra esigenza di sicurezza della cittadinanza e tutela della libertà dell'individuo*", come è ben sintetizzato in una sentenza della Corte suprema di Israele originata proprio dalla applicazione delle misure contro il terrorismo[81].

Più in generale si pone il problema di individuare *standard* di riferimento condivisi, fondati su regole giuridiche adeguate e aggiornate al mutato contesto tecnologico. Poiché il diritto segue l'evoluzione tecnologica, quasi mai la precede, si registra la tendenza in vari Stati a utilizzare vecchie regole ad un quadro di riferimento che nel frattempo è cambiato, applicando norme obsolete a tecniche di intercettazione che consentono, a differenza di una volta, un monitoraggio ampio e tendenzialmente onnicomprensivo, senza limiti di tempo e a costi limitati. Come rilevato, in alcuni Paesi l'utilizzo da parte delle autorità governative dei dati e delle informazioni raccolte non è disciplinato e l'insufficienza o l'inadeguatezza del regime giuridico crea, evidentemente, un terreno fertile per violazioni arbitrarie del diritto alla *privacy* e, di conseguenza, rischia di compromettere il diritto alla libertà di opinione e di espressione[82]. Talora la sorveglianza delle comunicazioni viene poi autorizzata senza un adeguato controllo giurisdizionale[83].

La principale questione che si pone è allora, da un lato, quella della verifica, in concreto, del *target* e delle modalità con cui tale sorveglianza si svolge, dall'altro quella dell'adeguatezza delle norme applicabili. E' alla stregua di esse, oltre che dei principi di proporzionalità e ragionevolezza, che deve valutarsi la legittimità di ogni

[80] *Conseil Constitutionnel, déc.* n. 94-352 DC *du* 18-1-1995.

[81] H.C.J. 5591/02, *Yassin v. Commander of Kziot Military Camp,* 18 dicembre 2002.

[82] Si veda *Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies*, adottata dal Comitato dei Ministri (Consiglio d'Europa) l'11 giugno 2013.

[83] Alcuni Stati, pur imponendo limiti temporali all'esecuzione degli ordini di intercettazione, consentono poi alle autorità incaricate dell'applicazione della legge di rinnovare tali ordini ripetutamente e indefinitamente.

intervento di monitoraggio e controllo[84]. Al riguardo rileva un insieme di previsioni normative nazionali, europee (Unione europea) e internazionali (Consiglio d'Europa e Nazioni Unite).

Il quadro giuridico vigente è alquanto variegato. Per esempio in Inghilterra l'intercettazione delle comunicazioni deve essere autorizzata dal Segretario di Stato, ma può essere effettuata anche al fine di salvaguardare il benessere economico ("*economic well-being*") del Paese (Sezione 5 *Regulation of Investigatory Powers Act*, 2000)[85]. In Colombia nel 2012 un decreto del governo (Ministeri della giustizia e delle tecnologie dell'informazione e della comunicazione) ha prescritto che i *service providers* realizzino un'infrastruttura alla quale la polizia giudiziaria possa accedere direttamente, senza previa autorizzazione del procuratore generale. In India nel 2012[86] è stato il governo a proporre di installare un sistema centralizzato di monitoraggio tale da indirizzargli tutte le comunicazioni, consentendo alle agenzie di sicurezza di aggirare l'interazione con i *service providers*. In Francia il potere esecutivo ha la possibilità di raccogliere i dati delle comunicazioni, senza alcun controllo giurisdizionale. Nel 1991 è stata istituita una Commissione per il controllo delle intercettazioni ("*Commission nationale de contrôle des interceptions de sécurité*"), ma ha soltanto il potere di adottare raccomandazioni sulla legalità delle intercettazioni, senza avere il potere di bloccarle. In Germania è consentita l'intercettazione di comunicazioni nazionali e internazionali da parte dei servizi di *intelligence* senza alcuna autorizzazione giudiziaria, laddove sia in questione la tutela dell'ordine democratico o la sicurezza dello Stato. In Svezia l'agenzia di *intelligence* nazionale è autorizzata per legge ad intercettare senza alcun mandato o ordine del tribunale tutto il traffico telefonico e internet che si svolge entro i confini del paese.

Con l'aumento dei flussi transnazionali di dati, poiché la raccolta dei dati prodotti sul territorio nazionale avviene spesso presso *service providers* collocati all'estero, gli Stati hanno incominciato ad estendere i propri poteri di sorveglianza al di fuori dei confini territoriali. Tale tendenza ha subito un'accelerazione nel corso del 2012, anno in cui gli Stati Uniti hanno emendato il *Foreign intelligence surveillance act* (FISA) del 2008, estendendo il potere del governo di sorvegliare i cittadini non-americani le cui comunicazioni siano ospitate da *cloud services*[87] collocati negli Stati Uniti (come quelli di Google e di altri giganti di internet) anche all'estero.

Occorre d'altronde considerare che, oltre che per la protezione dal rischio di attacchi terroristici, l'integrità dei sistemi informativi nazionali costituisce un

[84] Si veda M. D'AMICO, *La cooperazione di polizia e il problema delle intercettazioni di comunicazioni nell'area comunitaria*, in *La Comunità Internazionale,* n. 1/2001, 75-101.

[85] Oltre duecento agenzie governative, le forze di polizia e le autorità carcerarie sono autorizzate ad acquisire i dati delle comunicazioni ai sensi del *Regulation of Investigatory Powers Act* del 2000.

[86] F. LA RUE*, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, United Nations, General Assembly, 17 aprile 2013, par. 57.

[87] In tali casi non è sempre agevole sapere dove si trovino memorizzati i dati, chi abbia accesso agli stessi, chi sia responsabile del loro trattamento e quale tipo di processi di *back-up* e ripristino vengano messi in atto.

elemento chiave dell'interazione politica, sociale ed economica fra i paesi UE e la sicurezza (e quindi la protezione) di tali sistemi è fondamentale per lo sviluppo del mercato interno e di un'economia competitiva e innovativa. Come rilevato, attacchi informatici su larga scala possono infatti causare ingenti danni economici sia attraverso l'interruzione dei sistemi di informazione e di comunicazione sia mediante la perdita di dati o l'alterazione di informazioni commerciali importanti e riservate. In tal senso la tempestiva segnalazione e identificazione delle minacce e dei rischi derivanti da attacchi informatici, rese possibili dalla sorveglianza delle comunicazioni, sovente rappresentano elementi efficaci di prevenzione e costituiscono per certi aspetti la inevitabile risposta ai sempre più frequenti attacchi informatici e all'esigenza di migliorare la sicurezza dei sistemi informativi[88].

2.3. Le regole dell'Unione europea

Negli ultimi anni la questione della *cybersecurity* ha assunto una rilevanza strategica crescente per l'Unione europea[89], consapevole dell'importanza di disporre di un quadro giuridico elaborato con cura e aggiornato con tempestività, a beneficio anche degli Stati membri.

La prima importante iniziativa risale al 2001, con la comunicazione sulla criminalità informativa[90] adottata dalla Commissione, concernente la sicurezza delle infrastrutture dell'informazione e la repressione dei reati informatici, successivamente integrata dalla comunicazione, sempre del 2001, sulla "*network information security*"[91], da intendersi come "*la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema*" (par. 2.1).

Il *focus* europeo sul tema, atteso il fenomeno della crescente digitalizzazione dei sistemi, si era già palesato agli inizi degli anni 2000 con l'adozione di altre due comunicazioni, *e-Europe*[92] ed *e-Europe* 2005[93], che si collocavano nell'alveo della strategia elaborata dal Consiglio europeo nel marzo 2000 (cosiddetta strategia

[88] Si veda sulla problematica l'ampio ed accurato studio *Mass Surveillance*. *Part 1. Risks and opportunities raised by the current generation of network services and applications*. Scientific Foresight (STOA) Unit, Parlamento europeo, PE 527.409, gennaio 2015.

[89] N. KROES,*Working together to strenghten cybersecurity,* Speech 11/275, 15 aprile 2011.

[90] COM(2000) 890 del 26 gennaio 2001, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informativa*.

[91] COM (2001) 298 del 6 giugno 2001, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*. Questa comunicazione tipizzava le diverse minacce pregiudizievoli alla sicurezza delle reti, quali le intercettazione delle comunicazioni non autorizzate dall'autorità giudiziaria in base ai criteri normativi, l'accesso non autorizzato a computer e reti informatiche, i *disruptive attack* che determinano l'interruzione delle funzioni di un'infrastruttura critica con possibilità di danni economici gravi e l'esecuzione di *malware*.

[92] COM(2000) 130 dell'8 marzo 2000, *eEurope: Una società dell'informazione per tutti*.

[93] COM(2002) 263 del 28 maggio 2002, *eEurope 2005: una società dell'informazione per tutti*.

Lisbona 2000)[94] e dichiaratamente tesa a favorire lo sviluppo di un'economia di mercato "*più competitiva e più dinamica*"[95] con la necessità di aggiornare i servizi pubblici essenziali offerti sulle infrastrutture di rete. In questo contesto si colloca il "pacchetto" delle direttive del 2002 in tema di comunicazioni elettroniche, modificate nel 2009 dalla direttiva 2009/140/CE[96] (oltre che dalla 2009/136/CE), che impone agli Stati membri di approntare misure a livello nazionale che garantiscano la sicurezza delle reti[97].

Nel 2006, la "*Strategia per una società dell'informazione sicura*" individuava la sicurezza delle reti e dell'informazione nella "*capacità di una Rete o di un sistema d'informazione di resistere* […] *ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta Rete o sistema*"[98]. In tale contesto è fondamentale assicurare la protezione delle infrastrutture critiche informatizzate (cosiddette "CIIP"), che rappresentano anche *asset* funzionali all'operatività di altre. Segnatamente, le CIIP includono tutte le attività dei proprietari o dei gestori delle infrastrutture volte ad assicurare il loro funzionamento al di sopra di un livello minimo di servizio in caso di interruzioni, attacchi o incidenti.

Nella ripartizione delle competenze, occorre rilevare che sono gli Stati membri ad essere titolari delle principali responsabilità in tema di sicurezza[99], mentre all'Unione europea è affidato un ruolo sussidiario, di integrazione e armonizzazione delle iniziative nazionali. Ecco perché solo di recente l'Unione europea ha avviato iniziative rispondenti all'esigenza di delineare un quadro giudico efficace atto ad assicurare la sicurezza delle reti e delle informazioni attraverso la protezione delle infrastrutture critiche informatizzate, la lotta alla cyber-criminalità, la regolamentazione delle comunicazioni elettroniche (ivi inclusa la protezione della *privacy* e dei dati personali).

In materia ha anche individuato due obiettivi specifici da perseguire, in linea anche con le raccomandazioni contenute nella Strategia di sicurezza interna dell'UE

[94] Programma di riforme economiche approvato a Lisbona dai Capi di Stato e di Governo dell'Unione europea durante il Consiglio europeo del 23-24 marzo del 2000.
[95] *Ibidem*, p.7.
[96] Direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009, in GU L 337 del 18 dicembre 2009.
[97] Di tale "pacchetto" fa parte anche la direttiva 2002/58/CE, *e-privacy,* che si applica «[...] *al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione»* (art. 3, n.1) e prevede l'obbligo, per gli Stati membri, di assicurare la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione ed i servizi di comunicazione accessibili al pubblico, vietando in particolar modo «*l'ascolto, la captazione, la memorizzazione ed altre forme di intercettazione o di sorveglianza delle comunicazioni e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di quest'ultimi* [...]».
[98] Commissione europea, *Una strategia per una società dell'informazione Sicura - "Dialogo, partenariato e responsabilizzazione",* COM(2006) 656, Bruxelles, 3.
[99] Si vedano Art. 4, par. 2, TEU e Cons. 16, reg. UE 2016/679.

presentata il 22 novembre 2010 e nell'Agenda digitale europea avviata nell'agosto 2010[100]: (i) accrescere la consapevolezza dei principali rischi connessi alla *cybersecurity*; (ii) migliorare la preparazione e le capacità di risposta europee e nazionali a possibili attacchi o incidenti informatici.

Al fine di realizzare il primo obiettivo, la Commissione europea ha incoraggiato soprattutto il dialogo tra gli Stati membri e tra questi e le istituzioni europee, così come tra tutti gli *stakeholder* del settore, pubblici e privati. In quest'ottica, risulta strategica l'istituzione nel 2004 di una struttura *ad hoc*, quale l'Agenzia europea per la sicurezza delle reti e dell'informazione (*European Network and Information Security Agency*, ENISA), che rappresenta essenzialmente una piattaforma per lo scambio di informazioni e *best practices* tra istituzioni UE, autorità nazionali e imprese. Inoltre ha il compito di fornire pareri tecnici sia alle autorità degli Stati membri sia alle istituzioni europee[101].

Come accennato, la sicurezza dello spazio cibernetico concerne anche la sicurezza delle infrastrutture critiche su cui viaggiano i dati trasmessi in internet (il "*network* fisico"). L'Unione europea ha affrontato questo tema nel 2008 con la direttiva 2008/114/EC dell'8 dicembre, espressamente dedicata ai settori dell'energia e dei trasporti[102]. Per "*infrastruttura critica europea*" si intende quella il cui danneggiamento o distruzione comporti un impatto su almeno due Stati membri e la direttiva individua i criteri e stabilisce le procedure per l'individuazione di tali infrastrutture critiche delineando un primo livello generale per la predisposizione dei piani di sicurezza a cura dei proprietari/operatori di tali *asset* fisici.

Nel febbraio 2013, in collaborazione con l'Alto rappresentante dell'Unione europea per gli Affari esteri e la politica di sicurezza, la Commissione europea ha elaborato la propria strategia sulla sicurezza informatica contestualmente ad una proposta di direttiva in materia di sicurezza delle reti e dell'informazione: "*Uno spazio informatico aperto e sicuro*" (JOIN(2013)-1). Essa prevede azioni specifiche per rafforzare la resilienza e la capacità di recupero dei sistemi di informazione, ridurre la criminalità informatica e potenziare la politica internazionale dell'UE in materia di sicurezza e di difesa[103]. Accolta con favore dal Consiglio[104] e dal Parlamento

---

[100] Circa la strategia di sicurezza interna dell'UE, si veda Commissione europea, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, COM(2010) 673, Bruxelles.

[101] Regolamento (CE) 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, in G.U.U.E. 13 marzo 2004 L 077.

[102] Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, in G.U.C.E. 23 dicembre 2008 n. L 345. Tale strumento normativo è stato recepito in Italia con il decreto legislativo 11 aprile 2011, n. 61, in G.U. 102 del 4 maggio 2011. Si veda altresì la legge 7 agosto 2012, n. 133, modifiche alla legge 3 agosto 2007, n. 124, concernente il sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto, in G.U. 10 agosto 2012, n. 186.

[103] La strategia esprime la visione dell'UE in tema di sicurezza informatica, articolata in cinque priorità: conseguire la resilienza dei sistemi informatici; ridurre drasticamente la criminalità

europeo, essa pone l'accento, tra l'altro, sulla cooperazione tra il settore pubblico e quello privato per accrescere tale protezione.

Alla base della strategia europea vi è il concetto di *cyberresilience,* che si pone in antitesi rispetto all'idea di militarizzazione su cui si fonda principalmente la *cybersecurity* statunitense. La *cyberresilience* è figlia proprio della necessità di creare un *security framework* mirato alla prevenzione dei rischi basato su cooperazione e condivisione delle informazioni tra tutti gli attori coinvolti. Christou nel libro "*Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*"[105] si concentra proprio sull'importanza del concetto di *cyberresilience,* che si delinea in pratica secondo i seguenti criteri: (a) costruire una solida partnership tra Stati membri e istituzioni europee dedicate alla *cybersecurity* con l'obiettivo di condividere informazioni e individuare obiettivi e politiche comuni; (b) imporre standard, leggi e norme di sicurezza condivise; (c) promuovere lo sviluppo e la diffusione della cultura della *cybersecurity* a tutti i livelli.

La strategia europea del 2013 ha avuto il merito di proporre, per la prima volta, una nozione specifica di sicurezza cibernetica che include l'insieme delle misure cautelative e degli interventi che, al fine di preservare la disponibilità e l'integrità delle reti e delle infrastrutture e la riservatezza delle informazioni ivi contenute, possono essere approntate "*per proteggere il cyberdominio, in campo sia civile sia militare, nei confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti*"[106]. La strategia ha peraltro riconosciuto l'importanza essenziale delle tecnologie dell'informazione e della comunicazione, in particolare dei sistemi digitalizzati *lato sensu* e di internet, quali forza propulsiva della crescita degli Stati membri oltre che risorsa essenziale per il settore industriale.

Il 12 agosto 2013 è stata quindi adottata la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione[107], con l'obiettivo precipuo di armonizzare il diritto penale degli Stati membri con riferimento agli attacchi contro i sistemi di informazione. La stessa rileva che le rilevanti lacune e le differenze esistenti nel diritto e nelle procedure penali degli Stati membri possono ostacolare la lotta contro la criminalità organizzata e il terrorismo e rendere difficile un'efficace

---

informatica; sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune; sviluppare le risorse industriali e tecnologiche per la sicurezza informatica; istituire una coerente politica internazionale del cyberspazio per l'Unione europea e sostenere i valori fondamentali dell'UE.

[104] Conclusioni del 25 giugno 2013.

[105] G. CHRISTOU, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy,* Palgrave Macmillan, 2016.

[106] Strategia dell'Unione europea per la cybersicurezza: un cyberspazio aperto e sicuro, *cit*.

[107] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, in G.U.U.E. 14 agosto 2013, n. L. 218. Si veda ENISA, *The Directive on attacks against information systems. A Good Practice Collection for the implementation and application of this Directive*, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Workshop1/Jo_De_Muynck-ENISA-Octopus.pdf.

cooperazione di polizia e giudiziaria in materia. Di qui l'indicazione di *standard* minimi per la definizione dei reati, quali l'accesso illecito a sistemi di informazione (art. 3), l'interferenza illecita ai sistemi (art. 4) e ai dati (art. 5), l'intercettazione illecita (art. 6) e le relative sanzioni (artt. 9 e 11), la responsabilità delle persone giuridiche (art. 12), lo scambio di informazioni ed il miglioramento della cooperazione tra le autorità competenti, comprese le forze di polizia e gli altri servizi incaricati dell'applicazione della legge, nonché le pertinenti agenzie dell'Unione e gli organismi specializzati (art. 13)[108]. Mentre persegue l'armonizzazione dei reati e delle sanzioni su larga scala, la direttiva lascia agli Stati la determinazione degli interventi relativi agli attacchi di minore gravità. Un specifica previsione è poi dedicata alla giurisdizione[109], ove si rileva che la competenza è dei tribunali dello Stato sul cui territorio il reato è commesso o di cui l'autore è cittadino, "*quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso*". Inoltre, lo Stato è titolare della competenza giurisdizionale qualora "*a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato*". Alla luce delle peculiarità del reato, che non postula la presenza del reo sul territorio, si prevede per gli Stati la possibilità, previa comunicazione alla Commissione, di stabilire la competenza giurisdizionale per un reato commesso al di fuori del suo territorio, "*anche qualora: a) l'autore del reato risieda abitualmente nel suo territorio; o b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio*".

Meritevole di menzione anche la comunicazione della Commissione del 20 giugno 2014[110], sull'attuazione della strategia di sicurezza interna dell'UE per il periodo 2010-2014[111] che richiama, fra i cinque obiettivi strategici della strategia di sicurezza

[108] Per esempio *Eurojust*, *Europol* e *European Network and Information Security Agency* (ENISA).
[109] Art. 12, direttiva 2013/40/UE.
[110] Comunicazione della Commissione al Parlamento europeo e al Consiglio, Relazione finale sull'attuazione della strategia di sicurezza interna dell'UE per il periodo 2010-2014 Bruxelles, 20 giugno 2014, COM(2014) 365 final.
[111] La strategia di sicurezza interna (SSI) ("Verso un modello di sicurezza europeo", documento del Consiglio 5842/2/10) del 2010 era stata ideata per permettere all'Unione europea di reagire alle minacce esistenti ed emergenti e si propone di individuare le sfide in materia di sicurezza interna, tenendo conto del fatto che oggi molte delle sfide da affrontare sono di carattere transfrontaliero e intersettoriale che nessuno Stato membro è in grado, da solo, di rispondere efficacemente a queste minacce. La strategia individua inoltre principi e orientamenti comuni che, nel rispetto dei diritti fondamentali, rappresentano la base di un modello di sicurezza europeo e mirano all'ulteriore sviluppo di strumenti e politiche comuni utilizzando un approccio più integrato. La comunicazione della Commissione "Strategia di sicurezza interna dell'UE in azione" (COM(2010) 673) identifica i principali obiettivi strategici che l'UE e gli Stati membri devono perseguire per essere più efficaci nel prevenire e combattere le forme gravi di criminalità organizzata, il terrorismo e la criminalità informatica.

interna (SSI) 2010-2014, quello di aumentare i livelli di sicurezza per i cittadini e le imprese nel cyberspazio, rilevando come le nuove tecnologie abbiano offerto nuove opportunità agli attori del settore della sicurezza, al contempo creando tuttavia nuove minacce, inclusa quella della crescente espansione della criminalità informatica. Di qui la necessità di elaborare una risposta completa e adeguata, in termini di assetto normativo e meccanismi di cooperazione, per contrastare questo fenomeno[112].

Per una migliore tutela dei cittadini nei confronti della *cyber*-criminalità, *inter alia*, è stato istituito un Centro europeo per la lotta alla criminalità informatica (EC3), stabilito presso Europol, pienamente operativo dall'11 gennaio 2013[113], "[..] *in qualità di centro di sostegno operativo, investigativo e forense,* [dotato della] *capacità di mobilitare tutte le risorse degli Stati membri dell'UE necessarie a mitigare e ridurre le minacce provenienti dai criminali informatici, ovunque essi operino*", ha dichiarato Troels Oerting, Capo del Centro. Si tratta di un intervento che integra sul piano operativo specifici interventi legislativi, quali la già citata direttiva relativa agli attacchi contro i sistemi di informazione del 12 agosto 2013 (2013/40/UE) e quella relativa alla lotta contro lo sfruttamento sessuale dei minori e la pornografia minorile *on-line* del 2011[114] (2001/92/UE). L'EC3 è diventato un importante punto di riferimento in materia di criminalità informatica cooperando con gli Stati membri, Eurojust e paesi terzi in diverse indagini andate a buon fine[115]. Collabora inoltre con il settore privato mediante gruppi di consulenza nel campo della sicurezza di internet e dei servizi finanziari.

A livello internazionale, meritevole di menzione è anche la convenzione di Budapest sul *cybercrime*[116] del 23 novembre 2001, elaborata nell'ambito del Consiglio d'Europa. Entrata in vigore il 1° luglio 2004, costituisce tuttora un fondamentale punto di riferimento per la cooperazione internazionale nella lotta contro la

[112] Fra le azioni principali, quella di rafforzare la capacità di far fronte agli attacchi informatici, strumento di molte forme di reati. Secondo lo Speciale Eurobarometro sulla sicurezza informatica n. 404 del novembre 2013, i cittadini europei sono consapevoli di tale minaccia e il 76% dei residenti ritiene che il rischio di essere vittima di un reato informatico sia aumentato negli ultimi dodici mesi. "*Questo sondaggio mostra l'impatto devastante della cibercriminalità sull'utilizzo di Internet - troppe persone decidono di non sfruttare appieno tutte le possibilità offerte da Internet. A scapito sia della nostra economia digitale che delle nostre attività online. Dobbiamo rafforzare la cooperazione europea, partendo dal lavoro svolto dal Centro europeo per la lotta alla criminalità informatica, per mettere all'angolo la criminalità organizzata online*", ha dichiarato il Commissario UE per gli affari interni.

[113] Il Centro europeo per la lotta alla criminalità informatica (EC3) è stato inaugurato l'11 gennaio 2013. European Commission - IP/13/13, 9 gennaio 2013.

[114] Direttiva 2011/92/UE del Parlamento europeo e del Consiglio del 13 dicembre 2011 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio, in G.U.U.E. n. L. 26 del 28 gennaio 2012, recepita con decreto legislativo 4 marzo 2014, n. 39, in G.U. del 22 marzo 2014, n. 68. Il Parlamento europeo sostiene una legislazione più incisiva contro gli abusi sessuali sui minori, Commissione europea - IP/11/1255, 27 ottobre 2011.

[115] https://www.europol.europa.eu/sites/default/files/publications/ec3_first_year report.pdf

[116] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA &NT=185

criminalità informatica, nonché modello per le normative nazionali. Gli Stati firmatari si impegnano a combattere, anche mediante adeguati strumenti di indagine, ogni uso illecito del *web* volto ad alterare banche dati, diffondere virus informatici, provocare danni alla proprietà intellettuale e distribuire pornografia infantile. La Convenzione prevede che ciascuno dei firmatari qualifichi come reato le azioni volte a preparare, offrire, fornire, distribuire o ricevere materiali connessi alla pornografia infantile, così come la violazione dei diritti d'autore e dei diritti connessi ai sensi delle disposizioni internazionali vigenti. Si tratta del primo trattato internazionale sui reati commessi via internet, che l'Italia ha ratificato con legge 18 marzo 2008.

La Commissione europea e gli Stati Uniti hanno avviato nel 2012 l'Alleanza mondiale contro l'abuso sessuale di minori *online*, cui attualmente partecipano cinquantatré paesi, per una più efficace individuazione delle vittime e punizione dei colpevoli, attraverso una maggiore e sensibilizzazione e riduzione del materiale pedopornografico *online.*

Ai citati interventi si aggiungono poi una serie di iniziative di carattere operativo, volte a integrare i diritti fondamentali nel settore della sicurezza dell'UE. Per esempio, l'agenzia dell'UE per i diritti fondamentali (FRA) ha elaborato una serie di pareri[117] e relazioni[118] su questioni che vanno dalla protezione dei dati ai reati generati dall'odio fino alle forme di estremismo, e che influiscono anche sui profili riguardanti la sicurezza interna[119], individuando altresì specifici strumenti di intervento per i funzionari pubblici[120].

2.4. Un salto di qualità: la direttiva NIS e il *Cybersecurity Act*

Nel giugno 2007, due mesi dopo l'attacco all'Estonia, il ministro della difesa del paese baltico invocò regole per la cybersicurezza simili a quelle introdotte nel 1856 nel diritto marittimo che avevano posto fine alla pratica delle navi corsare. Il grido d'allarme rese evidente che occorreva uno sforzo, non più differibile, a livello internazionale ed europeo, per rendere affidabili e sicure reti, servizi e sistemi informativi e ricondurre alla disciplina del diritto fenomeni la cui diffusione e rilevanza rischiava di mettere in crisi un mercato vieppiù basato sull'interscambio dei dati, minando la fiducia di cittadini-consumatori e imprese.

[117] Disponibili all'indirizzo: http://fra.europa.eu/en/publications-and-resources/ opinions

[118] Disponibili all'indirizzo: http://fra.europa.eu/en/publications-and-resources.

[119] Nel dicembre 2013 la FRA ha presentato un manuale per la formazione delle forze di polizia basata sui diritti fondamentali (http://fra.europa.eu/en/publication/2013/fundamental-rights-based-police-training-manual-police-trainers), che integra un manuale relativo alla pratica discriminatoria della profilazione basata sull'etnia, che era stato pubblicato nel 2010 (FRA (2010) (*"Towards More Effective Policing, Understanding and preventing discriminatory ethnic profiling: a guide").*

[120] Si veda FRA (2013), *"Joining up fundamental rights. Toolkit for local, regional and national public officials"*.

Dopo aver definito nel 2008 il concetto di "infrastruttura critica europea"[121], ancorché limitato ai settori di energia e trasporti, lo sforzo dell'Unione europea giunge alfine a compimento nel 2016 con la direttiva NIS[122], che delinea un più ampio sistema integrato di soggetti pubblici e privati basato su responsabilità e compiti condivisi, definiti e verificabili, regole cogenti per settori specificamente indicati suscettibili di allargarsi ad altri in virtù del principio dell'"armonizzazione minima", oltre a *cybersecurity capabilities* adeguate.

Il progetto è ambizioso e la Commissione europea, nella Comunicazione del settembre 2017 dedicata alla NIS (un anno dopo la sua adozione), non ne fa mistero: occorre che la sua attuazione da parte degli Stati membri avvenga sulla base di un approccio armonizzato, ad evitare disallineamenti e frammentazioni tali da comprometterne gli obiettivi. Di qui una serie di indicazioni concrete per gli Stati membri in vista delle scadenze del 9 maggio e del 9 novembre 2018, rispettivamente per la sua trasposizione e la designazione degli operatori dei servizi essenziali che gestiscono infrastrutture critiche per la sicurezza nazionale.

Con la NIS la cybersicurezza entra a far parte a pieno titolo del lessico europeo. Termina la fase in cui gli Stati, in virtù degli ampi margini di manovra che consentiva loro la nozione di "sicurezza nazionale" sono liberi di muoversi con disinvoltura e ne incomincia una nuova, fatta di previsioni puntuali, coordinamento e interazione, sotto la guida della Commissione europea. Lo impongono le regole di un sistema ormai integrato che in quello stesso anno, il 2016, vede Europa e Stati Uniti riprendere il dialogo, con l'accordo sul *Privacy Shield* raggiunto dopo mesi di tensione seguita alla sentenza sul caso Schrems[123] e il rilevante allineamento normativo compiuto dagli USA ai più rigorosi parametri europei. *Privacy* e cybersicurezza sono ormai due facce della stessa medaglia, strettamente collegate.

Il 2016 è anche l'anno in cui viene adottato il "pacchetto" europeo in tema di protezione dati personali, con il regolamento applicabile dallo scorso 25 maggio, pietra miliare e *best practice* a livello internazionale, frutto di un complesso e articolato processo di adozione.

La NIS non è pertanto solo il primo insieme organico di norme in tema di cybersicurezza, ma l'elemento centrale di un cantiere normativo in corso che vede tuttora impegnati vari attori, a vari livelli e su vari fronti.

In primis gli Stati membri che, scaduto qualche giorno fa il termine per la trasposizione, sono ora impegnati nella individuazione degli operatori dei servizi essenziali sotto l'occhio vigile della Commissione europea; quindi il Consiglio

[121] Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, in GU L 345 del 23 dicembre 2008.

[122] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, in GU L 194 del 19 luglio 2016.

[123] Sentenza della Corte (Grande Sezione) del 6 ottobre 2015, Maximillian Schrems contro Data Protection Commissioner, causa C-362/14.

d'Europa, che ha da qualche giorno concluso la revisione della convenzione n. 108 del 1981, speculare al RGPD europeo. Protagonista della scena è tuttavia l'Unione europea, che con la NIS torna ad assumere il ruolo di guida e stimolo a lungo atteso. Dopo le misure del pacchetto *Privacy* del 2016, sta aggiornando le regole sull'*E-privacy* per le comunicazioni elettroniche e, con le iniziative del 13 settembre 2017, *in primis* il *Cybersecurity Act* e il previsto sistema di certificazione, ha posto le basi del futuro mercato europeo della cybersicurezza.

Gli strumenti sono diversi ma gli obiettivi convergono: l'affidabilità e sicurezza delle attività economiche e sociali: gli stessi che sono alla base della NIS, che si rivela quindi tassello fondamentale del complesso e articolato mosaico che l'Unione europea sta poco a poco componendo. Ne sono oggetto reti, sistemi, servizi informativi e dati personali, sempre più strettamente interconnessi.

Nel 2016 la Commissione europea ha adottato una comunicazione[124] dedicata espressamente a rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cybersicurezza. A ciò si aggiunge un piano per l'avvio di un partenariato europeo pubblico-privato per la sicurezza informatica, con la partecipazione di pubbliche amministrazioni nazionali, regionali e locali, centri di ricerca e università. L'obiettivo è quello di promuovere la cooperazione fin dalle prime fasi della ricerca e dell'innovazione e a sviluppare soluzioni di cybersicurezza per settori quali l'energia, la sanità, i trasporti e la finanza.

Nello stesso anno, come rilevato, sono stati adottati il cosiddetto "*pacchetto Privacy*", composto dal regolamento in tema di protezione dei dati personali 2016/679 (RDPD), applicabile a partire dal 25 maggio 2018, la direttiva *Enforcement* 2016/680, che regola il trattamenti dei dati personali nei settori della prevenzione, contrasto e repressione dei crimini, trasposta con d. lgs. 18 maggio 2018, n. 51 e la direttiva 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, trasposta con d. lgs. 21 maggio 2018, n. 53.

Ma è la direttiva NIS 2016/1148, trasposta con il d.lgs. n.65 del 18 maggio 2018, a costituire il tassello più rilevante del mosaico normativo europeo. Si tratta infatti del primo insieme organico di norme in tema di sicurezza informatica e rappresenta un passaggio cruciale per la costruzione di un sistema di sicurezza europeo, secondo quanto preconizzato nel 2013 nella comunicazione congiunta di Commissione, Parlamento e Consiglio, su "*Cybersecurity strategy of the European Union: an open, safe and secure cyberspace*"[125].

Con tale direttiva termina la fase in cui gli Stati, in virtù degli ampi margini di manovra che dava loro la nozione di "sicurezza nazionale" (concetto alquanto

[124] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cybersicurezza, 5 luglio 2016 COM(2016) 410 final,

[125] Bruxelles, 7 febbraio 2013 JOIN(2013) 1 final.

indefinito, sia a livello internazionale sia europeo), sono liberi di muoversi con una disinvoltura e ne incomincia una nuova, fatta di regole puntuali e di coordinamento. Tutto ciò è evidentemente necessario per un mercato digitale e un'economia interconnessa (a cui si rivolgono le iniziative del *Digital Single Market* e lo stesso "*pacchetto Privacy*" adottato il 27 aprile 2016) che ha nel traffico dati uno dei suoi elementi chiave e che viene quotidianamente messa a dura prova da cyber-attacchi e criminalità.

I soggetti riguardati sono gli operatori di servizi essenziali e i fornitori di servizi digitali operanti nei settori rispettivamente indicati negli allegati II (energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali) e III (mercato *online*, motore di ricerca online, *cloud computing*) della direttiva. Mentre i primi debbono essere identificati dagli Stati membri (il termine era fissato al 9 novembre 2018[126]), i fornitori di servizi digitali sono individuati attraverso un duplice richiamo alla direttiva 2015/1535, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione[127].

La direttiva impone un livello minimo di sicurezza per le tecnologie, le reti e i servizi digitali in tutti gli Stati membri, garantendo parità di condizioni tramite norme armonizzate, impone a tutti gli Stati membri, alle aziende internet e agli operatori di infrastrutture principali, a piattaforme di e-commerce, reti sociali e servizi in materia di trasporti, banche e assistenza sanitaria, di garantire un ambiente digitale sicuro e affidabile. Ha quali obiettivi precipui il rafforzamento della sicurezza e della resilienza informatica all'interno del territorio dell'Unione europea, attraverso un approccio teso alla predisposizione di standard minimi in tema di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza senza pregiudicare la possibilità, per gli operatori di servizi essenziali e i fornitori di servizi digitali, di applicare misure di sicurezza maggiormente prescrittive.

Con riferimento al diverso aspetto dei controlli all'esportazione delle tecnologie di cyber-sorveglianza, nel settembre del 2016 la Commissione ha proposto[128] la modifica del regolamento (CE) n. 428/2009 del Consiglio sul controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso civile e militare[129]. La proposta si muove lungo due direttrici: (i) ampliare la definizione di "*prodotti a duplice uso*"[130] alle tecnologie di cyber-

[126] Vedasi Airpress, n. 07/2016, 8.

[127] Art. 4, nn. 5) e 6), *id*.

[128] Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un regime dell'Unione di controllo delle esportazioni, del trasferimento, dell'intermediazione, dell'assistenza tecnica e del transito di prodotti a duplice uso, COM(2016) 616 final del 28 settembre 2016.

[129] GU L 134 del 29 maggio 2009.

[130] L'articolo 2 della proposta definisce i "prodotti a duplice uso" come "*i prodotti, inclusi il software e le tecnologie, che possono avere un utilizzo sia civile sia militare; essi comprendono: a) prodotti che possono essere impiegati per la progettazione, lo sviluppo, la produzione o l'uso di armi nucleari, chimiche e biologiche e dei loro vettori, compresi tutti i prodotti che possono avere sia un utilizzo non esplosivo sia un qualche impiego nella fabbricazione di armi nucleari o di altri congegni esplosivi*

sorveglianza, qualora si verifichino casi di gravi violazioni dei diritti umani o del diritto internazionale, oppure in presenza di minacce per la sicurezza internazionale o per gli interessi essenziali di sicurezza dell'Unione e dei suoi Stati membri; e (ii) agevolare i controlli sui trasferimenti tecnologici, garantendo un elevato livello di sicurezza e trasparenza per evitare un utilizzo anomalo delle esportazioni[131].

Con il cosiddetto "*pacchetto Cybersicurezza*" del 13 settembre 2017 la Commissione europea, insieme all'Alto Rappresentante, ha aggiornato e rafforzato la propria strategia mediante una serie di diversi strumenti giuridici[132], di cui alcuni immediatamente operativi, altri che lo diventeranno non appena saranno approvati all'esito della procedura legislativa avviata. Si tratta di una raccomandazione, due comunicazioni, una proposta di regolamento e una proposta di direttiva.

Preannunciata dal Presidente Juncker nel discorso sullo "Stato dell'Unione", l'iniziativa si pone l'obiettivo di aumentare la resilienza dell'UE nei confronti degli attacchi *cyber* per proteggere il nascente mercato unico della cybersicurezza con interventi concreti con un assetto istituzionale rafforzato, a livello europeo e nazionale. La strategia della Commissione è basata sul ruolo dell'ENISA, il cui mandato viene reso permanente e a cui vengono attribuiti nuovi compiti e risorse per assumere un ruolo più direttamente operativo (quindi non più solo di mera consulenza) a supporto di Commissione e Stati membri; un quadro di regole per una certificazione di sicurezza EU di prodotti ICT, sistemi e servizi, fondato su *standards* internazionali e su base volontaria; il *Blueprint*, vale a dire principi e meccanismi (in termini di obiettivi e modalità di cooperazione) per rispondere in modo coordinato a incidenti e crisi *cyber* su larga scala; la proposta di creare una rete europea e un centro di ricerca e competenza in tema di *cyber* sicurezza. A ciò si aggiunge una proposta di direttiva per combattere la frode e la contraffazione degli strumenti di pagamento non in contanti (carte di credito e debito) per fornire una risposta efficace, dal punto di vista dell'intervento repressivo e del diritto penale, focalizzata

---

nucleari; b) tecnologia di sorveglianza informatica che può essere impiegata per commettere gravi violazioni dei diritti umani o del diritto umanitario internazionale, o che può rappresentare una minaccia per la sicurezza internazionale o gli interessi essenziali in materia di sicurezza dell'Unione e dei suoi Stati membri".

[131] Già nel dicembre 2014 la Commissione aveva adottato un regolamento delegato che modificava il regolamento (CE) 428/2009 aggiungendo alla categoria dei "prodotti a duplice uso" anche i "software di intrusione", ossia quei programmi per elaboratore che permettono l'accesso "segreto" ai sistemi di informazione e di telecomunicazione. Si veda il regolamento delegato (UE) 1382/2014 della Commissione del 22 ottobre 2014, che modifica il regolamento (CE) 428/2009 del Consiglio che istituisce un regime europeo di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso, in GU L 371 del 30 dicembre 2014.

[132] Joint Communication. Resilience, Deterrence and Defence JOIN (2017)450 final, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') COM(2017)477 final, Communication Making the most of NIS COM(2017)476 final and its Annex, Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA COM(2017)489 final, Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (The Blueprint) S(2017)6100 final.

sulla rilevazione, tracciabilità e repressione dei *cyber* criminali coinvolti in attività che per lo più hanno una dimensione transnazionale quali terrorismo, traffico di droga e di esseri umani. Della serie di interventi fanno parte anche misure volte a rafforzare la cooperazione internazionale in tema di *cyber* sicurezza e per una risposta diplomatica congiunta UE alle attività *cyber* dannose. Di particolare rilievo la comunicazione dedicata alla direttiva NIS[133], a cui è allegato un documento ricco di indicazioni operative per la sua trasposizione, avvenuta con d.lgs. n. 65/2018[134], entrato in vigore il 24 giugno 2018.

2.5. Le nuove sfide: il contrasto alla "minaccia ibrida"

La cosiddetta "minaccia ibida" è sempre più al centro delle preoccupazioni dell'Unione europea così come dei nostri servizi di sicurezza. Se nella Relazione 2016 "*la variabile cibernetica*" come strumento di offesa incominciava a delinearsi tramite "*azioni informali, discontinue, apparentemente occasionali*", sovente inserite in vere e proprie campagne di guerra asimmetrica con attacchi seriali e tattiche operative tali da rendere difficile risalire agli aggressori (Premessa, pag. 16), nella Relazione sulla politica dell'informazione per la sicurezza 2017 presentata il 20 febbraio 2018 assume invece le caratteristiche di una realtà sempre più "*perniciosa, sofisticata e di difficile rilevazione*". Insomma, lo strumento cibernetico agevola attività di influenza realizzate attraverso *"la manipolazione e la diffusione mirata di informazioni preventivamente acquisite attraverso manovre intrusive nel cyber-spazio*". Si tratta delle cosiddette *Fake News*, volte ad orientare l'opinione pubblica, fomentare tensioni socio-economiche, accrescere l'instabilità politica dei paesi occidentali, soprattutto in occasione dell'adozione di decisioni strategiche (Allegato alla Relazione).

Con precisione ed efficacia il Direttore del DIS individua pertanto una minaccia che non ha precedenti, almeno nel nostro paese, che è al tempo stesso pericolosa e subdola in quanto apparentemente inoffensiva, incide sui meccanismi di formazione del consenso, condiziona la libertà di espressione ed è potenzialmente destabilizzante per lo stesso sistema democratico. Se si considera che Google da solo può influenzare circa un quarto dell'elettorato, secondo le stime di Robert Epstein dell'*American Institute for Behavioral Research and Technology*, e che dall'analisi dei *Big Data* tratti dal *web* società come *Cambridge Analitica* sono in grado di delineare con precisione abitudini quotidiane, preferenze alimentari, financo orientamenti politici e tendenze sessuali, prevedendo il comportamento di chiunque, ci si rende conto che il tema non può essere sottovalutato.

[133] COM(2017)476 final.

[134] Decreto legislativo 18 maggio 2018, n. 65, attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, in GU Serie Generale n.132 del 9 giugno 2018.

Il tema *Fake News* è da tempo all'esame della Commissione europea[135], che ha concentrato i propri sforzi per fronteggiare le campagne mirate di disinformazione poste in essere con per o più non convenzionali, insidiose e difficili da contrastare in quanto in continua evoluzione. Incidono infatti sull'opinione pubblica e la rendono vulnerabile, alterando i meccanismi di formazione del consenso e lo stesso processo democratico.

Loro strumento precipuo sono i *social networks*, ormai considerati ambienti virtuali rilevanti ai fini della sicurezza nazionale e dei relativi interessi strategici, piattaforma ideale per l'avvio di campagne di disinformazione condotte sovente da paesi terzi attraverso *hackeraggio* di reti, tecniche che comprendono la manipolazione di video o documenti ufficiali, *bot e troll,* campionario di una nuova *warfare* non meno cruenta di quella tradizionale.

Di qui la necessità per l'Unione europea di disporre di un quadro giuridico[136] accurato e aggiornato che permetta agli Stati membri di intervenire per sanzionare gli autori di questi attacchi, con la consapevolezza che risulta talora difficile attribuirne con certezza la responsabilità, che si tratti di privato o attore statuale.

Al centro dell'attenzione soprattutto il processo elettorale, da mettere in sicurezza per consentire l'esercizio di un diritto e salvaguardare altresì la credibilità dei candidati, esposti al rischio di attacchi cyber volti a minarne la reputazione. Occorre, secondo la Commissione, un patto coinvolga autorità pubbliche e operatori privati, a beneficio dei cittadini e della loro capacità di discernimento, basato su una serie di strumenti per contrastare chi lucra sulla disinformazione alterando i messaggi elettorali magari attraverso video falsi (anche solo parzialmente) ma verosimili per screditare o mettere in cattiva luce gli avversari politici. Le più recenti applicazioni dell'intelligenza artificiale e del *machine learning* rendono infatti pressoché impossibile distinguere prodotti audio-video contraffatti senza l'ausilio di adeguati strumenti tecnici

[135] Meritevole di menzione, fra le varie proposte volte a fronteggiare il problema, quella formulata da Dan Shefet durante l'audizione al Senato francese il 15 febbraio 2019. Lo studioso propone che Facebook e gli altri *Social Media* siano obbligati ad abilitare un algoritmo che, al raggiungimento di una determinata "massa critica" di utenti (es. diecimila) che segnalano come controversa una notizia, entro 48 ore la evidenzi con un "tag" riconoscibile da tutti gli utenti. In tal modo si evita ai *Social* di operare una qualche forma di censura o rimozione dal *web*, rendendo edotti gli utenti che c'è qualcosa che non va nella notizia in cui si imbattono. Un ulteriore e temibile rischio per la democrazia, a ben vedere, oltre alle "*Fake news*" in sè, termine improprio a cui dovrebbe sostituirsi quello di "notizie controverse", è rappresentato dalle "notizie selettive", differenziate a seconda dei destinatari in relazione al loro profilo. Al riguardo il rimedio proposto da Shefet appare di particolare interesse: vietarle almeno nel periodo che precede le elezioni. In sostanza, l'informazione sul *web* non dovrebbe essere "targettizzata" e le cosiddette "bolle" (peraltro funzionali a legittimi interessi commerciali) sono da disabilitare prima delle consultazioni elettorali così che ogni cittadino riceva le stesse notizie, ad evitare che sia sottoposto ad indebiti condizionamenti.

[136] L'esigenza era già stata evidenziata dal Consiglio europeo del 2015, dalla comunicazione del 6 aprile 2016, dal Summit di Bruxelles del 18 ottobre 2018 e in occasione della conferenza EPSC "*Election interference in the digital age*" a Bruxelles il 15 e 16 ottobre 2018.

La comunicazione della Commissione europea del 26 aprile 2018[137] e il "*Code of practice*" del 26 settembre 2018 affidano un ruolo chiave alla società civile e alle piattaforme digitali, che sono invitate a utilizzare indicatori per verificare la credibilità delle fonti informative e impegnarsi a rendere più trasparenti i messaggi di propaganda elettorale su di esse veicolati.

Il 5 dicembre 2018 è stato adottato dalla Commissione il rapporto sull'applicazione della comunicazione del 26 aprile 2018[138] e la comunicazione congiunta (insieme all'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza) per un piano d'azione contro la disinformazione[139].

Il "*Compendium on Cybersecurity of Election Technology*", pubblicato nel marzo 2018 sotto l'egida del Gruppo di cooperazione della direttiva NIS 2016/1148, costituisce una guida completa ed accurata delle misure volte a proteggere la segretezza, la disponibilità e l'integrità dei sistemi di voto e dei dati personali coinvolti nel processo elettorale (per esempio, la registrazione dei votanti e dei candidati, la raccolta delle schede, lo spoglio dei voti e la trasmissione dei risultati). Al fine di rafforzare lo "scudo protettivo" è stato anche proposto di applicare al processo elettorale misure tecnico-organizzative "adeguate" alla gestione dei rischi e alla prevenzione degli incidenti informatici secondo i meccanismi della direttiva NIS in presenza di un'"infrastruttura critica nazionale" o un "servizio essenziale".

L'obiettivo è di predisporre gli strumenti più adeguati per una risposta coordinata, a tutela di un ecosistema on-line trasparente, affidabile e responsabile, per garantire libertà di espressione e un corretto processo democratico. Di qui l'invito alla mobilitazione dei vari attori istituzionali sulla base di una serie di misure raccolte intorno a quattro "pilastri": rafforzare la capacità UE (con risorse aggiuntive, esperti dedicati alla rilevazione e all'analisi dei rischi, una comunicazione strategica rafforzata), mettere a punto meccanismi di coordinamento (con un sistema di allarme rapido e un unico punto di contatto nazionale, una cooperazione rafforzata UE-Stati membri), mobilitare il settore privato sulla base del citato codice di autoregolamentazione del 26 settembre 2018 con il coinvolgimento di piattaforme *on-line*, industria pubblicitaria, operatori media e l'identificazione dei falsi account, aumentare la consapevolezza e la capacità di reazione della società civile (per verificare l'origine della disinformazione con una rete di *fact checkers* indipendenti e l'ausilio di un giornalismo di qualità per un'opinione pubblica informata e consapevole).

---

[137] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Contrastare la disinformazione online: un approccio europeo", 26 aprile 2018 COM(2018) 236 final.

[138] Relazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sull'attuazione della comunicazione "Contrastare la disinformazione online: un approccio europeo", 5 dicembre 2018 COM(2018) 794 final.

[139] Comunicazione congiunta al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Piano d'azione contro la disinformazione, 5 dicembre 2018 JOIN(2018) 36 final.

Come rilevato, il tema della disinformazione riveste una particolare delicatezza e rilevanza, perché inerisce all'essenza stessa della democrazia. Incide sulla formazione dell'opinione pubblica, riguardando la libertà di espressione e di stampa, vale a dire la libertà di informare e di essere informati che è garantita dall'articolo 21 della Costituzione ed è insuscettibile di limitazione, se non alla stregua di quanto previsto dalla medesima previsione così come precisato dalla consolidata giurisprudenza della Corte Costituzionale.

Tuttavia nessun intervento volto a contrastare la disinformazione può incidere sulla libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, in quanto inviolabili e non soggetti a limitazione se non su atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge, ai sensi l'articolo 15 della nostra Costituzione.

Ancorché nel rapporto del novembre 2018 "*News vs fake nel sistema dell'informazione*" l'Autorità per le garanzie nelle comunicazioni abbia rilevato che le fonti informative online (siti di quotidiani, testate online, social network), a parità di risorse professionali utilizzate, producano una maggiore offerta di informazione, il fenomeno della diffusione di notizie false non riguarda solo la rete, ma il sistema dell'informazione e della comunicazione nel suo complesso, ivi compresi i *mass media* tradizionali.

Concetti quali "informazione ingannevole", "disinformazione" e "notizie false" hanno diverse accezioni; rivestono una particolare pericolosità nuove forme di contenuti audio o video artificiali, realistici e generati tramite IA, noti come "media artificiali" (i cosiddetti *deep fake*) in quanto in grado di manipolare l'informazione e condizionare l'opinione pubblica e che possono essere rilevati per lo più solo con appositi strumenti tecnici e operativi. Il problema ha assunto una particolare rilevanza in Europa durante l'emergenza Covid-19.

Sul tema è stata istituita un'apposita Commissione parlamentare d'inchiesta sulla diffusione intenzionale, seriale e massiva di informazioni false, attualmente al lavoro in Italia. Inoltre già opera a livello europeo EUvsDisinfo, una task force per la lotta alla disinformazione del Servizio UE per l'azione esterna (SEAE), che da qualche mese ha concentrato la propria attenzione sui casi di disinformazione relativi al Covid-19, raccolti in un database costantemente aggiornato.

3. IL 5G, FRA MISURE TECNICHE E REGOLAMENTARI

Quella che si sta giocando sulla tecnologia e le reti di quinta generazione è una partita dalle molteplici implicazioni, che ha preso le mosse da profili essenzialmente tecnici ed economici per assumere sempre più una dimensione di carattere politico e strategico. D'altronde - come rileva la Commissione europea nella raccomandazione del 26 marzo 2019 – l'importanza del 5G risiede nel fatto che si tratta della futura colonna portante della società e dell'economia, in grado di collegare oggetti e sistemi anche in ambiti critici come l'energia, i trasporti, le banche e la salute, nonché gli apparati di controllo che veicolano informazioni sensibili che sono alla base dei sistemi di sicurezza.

3.1. La tecnologia e la rete di quinta generazione

Dal punto di vista tecnico la connettività pervasiva e l'automazione intelligente indotta dal 5G consentono non solo un notevole aumento della capacità di banda e quindi della velocità di trasmissione per i terminali radiomobili (*bitrate*), ma anche la disponibilità di una vasta gamma di servizi interattivi ad alta affidabilità basati sull'operatività in *real time* (bassa latenza). La copertura di rete richiederà celle di dimensioni più ridotte (*small cell)* ma in numero maggiore rispetto a quelle attuali. Occorre quindi installare più antenne alimentate da collegamenti fisici, come le fibre ottiche, in grado di assicurare una più elevata capacità di banda[140].

Questo si traduce nella necessità di realizzare collegamenti in fibra ottica in maniera capillare e diffusa sul territorio, come sta avvenendo nei centri urbani con lo sviluppo di reti di accesso interamente ottiche (FTTH, *fibre to the home* e FTTB, *fibre to the building*). Nelle zone rurali, invece, il 5G sarà complementare alla rete fissa per assicurare la copertura *ultrabroadband* dei piccoli centri grazie all'utilizzo della tecnologia FWA (*fixed wireless access*). La necessità per gli operatori di contenere gli investimenti, in particolare dopo aver sostenuto gli ingenti costi per l'acquisto delle licenze[141] (in Italia la gara si è conclusa il 2 ottobre 2018 con un introito per lo Stato

[140] Con la decisione n. 243/2012/UE del 14 marzo 2012, è stato definito un programma pluriennale europeo in materia di spettro radio ("*Radio Spectrum Policy Programme*"- RSPP), che prevede che gli Stati membri e la Commissione europea cooperino per sostenere e conseguire una serie di obiettivi strategici, in particolare che adottino tutte le misure necessarie per garantire la disponibilità di spettro radio sufficiente (almeno 1.200 Mhz) per copertura e capacità all'interno dell'Unione, al fine di consentire di disporre della banda larga più veloce e fare in modo che le applicazioni senza fili ed il ruolo guida europeo nei nuovi servizi possano contribuire efficacemente alla crescita economica e alla realizzazione dell'obiettivo dell'accesso ad una velocità della banda larga di almeno 30 Mbps entro il 2020 per tutti cittadini (Risoluzione del Parlamento europeo del 19 gennaio 2016). La comunicazione della Commissione del 6 maggio 2015 "*A Digital Single Market Strategy for Europe*" e la successiva la comunicazione, c.d "*Gigabit Society*" del 14 settembre 2016, hanno evidenziato che la disponibilità di un idoneo quantitativo di spettro radio rappresenta uno dei presupposti essenziali per la fornitura e diffusione dei servizi *wireless* a banda larga e ultra-larga, insieme ad adeguati standard a garanzia di una comunicazione efficiente tra i vari componenti digitali (quali dispositivi, reti e archivi di dati), sottolineando l'importanza delle reti di telecomunicazione ad alta capacità, ritenute un asset fondamentale affinché l'Unione europea possa competere nel mercato globale.

[141] Dai sito web del Ministero dello sviluppo economico: "Roma, 2 ottobre 2018. Oggi, alle ore 17.30, si è chiusa la procedura per l'assegnazione dei diritti d'uso delle frequenze per il 5G avviata il 13 settembre. Le procedure di gara hanno portato ad una competizione vivace, conclusasi in 14 giornate di miglioramenti competitivi e con 171 tornate. L'introito raggiunto ha superato del 164% il valore delle offerte iniziali e del 130,5% la base d'asta. L'ammontare totale delle offerte per le bande messe a gara ha raggiunto i 6.550.422.258,00 euro, superando di oltre 4 miliardi l'introito minimo fissato nella Legge di Bilancio. In particolare: lotti per la banda 700 MHz FDD hanno raggiunto la quota di 2.039.909.188,00 euro; i lotti per la banda 3700 MHz hanno raggiunto quota pari a 4.346.820.000,00 euro; i lotti per la banda 26 GHz hanno raggiunto la quota di 163.693.070,00 euro. Nessuna offerta è stata fatta per i lotti 700 MHz SDL, pertanto i soggetti che ne abbiano manifestato l'interesse potranno partecipare alla fase di gara successiva, secondo le procedure previste dal disciplinare di gara per frequenze non aggiudicate, che si svolgerà a partire da venerdì 5 ottobre. Il lotto riservato ai nuovi entranti di 10 MHz in banda 700 MHz FDD è stato aggiudicato dal remedy taker Iliad Italia S.p.A. per 676.472.792,00 euro, mentre Vodafone S.p.A. si è aggiudicato 2 lotti generici in banda 700 MHz FDD, per un totale di 10 MHz alla cifra complessiva

di oltre 6 miliardi e mezzo di euro), induce inevitabilmente a cercare sinergie non solo con lo sviluppo della rete fissa di accesso in fibra, ma anche a condividere l'infrastruttura delle nuove *small cells* evitando i costi di duplicazione per il dispiegamento delle antenne 5G[142].

Di qui la necessità di una regolazione adattiva e *business friendly* che possa ovviare alle problematiche che collocano il nostro paese al 23° posto (su 38) secondo il *5G Readiness Index* 2019 elaborato da inCites Consulting; a dispetto di una positiva valutazione in termini di "*Infrastructure and Technology*"(4° posto), l'assetto normativo viene giudicato inadeguato per il rapido sviluppo delle reti 5G (al punto da far scivolare l'Italia al 35° posto nella classifica per "*Regulation and Policy*").

La rete 5G costituisce insomma una piattaforma tecnologica strategica per lo sviluppo di un paese ad economia avanzata e tramite essa saranno erogati molti servizi essenziali, specializzati e calibrati in base delle specifiche esigenze dei

---

di 683.236.396,00 euro. I restanti 2 lotti generici in banda 700 MHz FDD, per un totale di 10 MHz, sono stati aggiudicati da Telecom Italia S.p.A. per un importo complessivo di 680.200.000,00 euro. I 5 lotti in banda 26 GHz sono stati aggiudicati 1 per ogni società: in particolare Telecom Italia S.p.A. si è aggiudicata un lotto per 33.020.000,00 euro, Iliad Italia S.p.A. si è aggiudicata un lotto per 32.900.000,00 euro, Fastweb S.p.A. si è aggiudicata un lotto per 32.600.000,00 euro, Wind 3 S.p.A. si è aggiudicata un lotto per 32.586.535,00 e Vodafone Italia S.p.A. si è aggiudicata un lotto per 32.586.535,00 euro. La fase dei miglioramenti competitivi ha visto una vivace competizione da parte delle società partecipanti in particolare sulla banda 3700 MHz. A valle di tale competizione la società Telecom Italia S.p.A. si è aggiudicata il lotto specifico (C1) di 80 MHz per 1.694.000.000,00 euro, la società Vodafone Italia S.p.A. si è aggiudicata il lotto generico di 80 MHz per 1.685.000.000,00 euro, la società Wind 3 S.p.A. si è aggiudicata un lotto generico di 20 MHz per 483.920.000,00 euro e la società Iliad Italia S.p.A. si è aggiudicata il secondo lotto generico di 20 MHz per 483.900.00. Cfr. https://www.mise.gov.it/index.php/it/198-notizie-stampa/2038666-gara-5g.

[142] […] Nell'aprile 2019, la Corea del Sud è stato il primo paese ad avviare commercialmente il 5G su una scala più ampia e, a dicembre 2019, circa 5 milioni di coreani avevano telefoni 5G. Il più grande lancio commerciale nel 2019 è avvenuto in Cina, che ha dispiegato oltre 100.000 stazioni base in oltre 50 città a novembre e si prevede che raggiungerà 143 milioni di utenti 5G nel 2020. In effetti, a questo ritmo, molti si aspettano che la Cina dominerà il mercato globale del 5G entro il 2025. Gli Stati Uniti e il Giappone cresceranno rapidamente nell'adozione del 5G, mentre l'UE rimarrà indietro. Dal punto di vista industriale, due delle cinque società che servono lo spazio della rete di accesso radio 5G sono europee: Ericsson e Nokia. Secondo alcuni analisti, in un mondo digitale sempre più dominato da società cinesi e statunitensi, il 5G è uno dei pochi mercati futuri in cui i fornitori europei sono in una posizione molto favorevole per competere con queste aziende sin dall'inizio. […] Attualmente, il 5G è nella sua prima fase di attuazione (ovvero "non autonomo" (NSA), supportato dall'infrastruttura di rete radio e core esistente a lungo termine (LTE) (4G)). Tuttavia, il 4G sta iniziando a esaurire la capacità a causa dell'esplosione del traffico dati mobile e il passaggio al 5G autonomo è necessario per far fronte a questa tendenza. […] Il primo intervento di chirurgia cerebrale remota umana abilitato al 5G si è svolto in Cina lo scorso novembre, con medico e paziente distanti oltre 2400 km. Secondo l'International Telecommunication Union (ITU), gli standard che supportano tutte le applicazioni 5G saranno in vigore nel 2020. Alcuni fornitori di servizi di telecomunicazione preferiscono passare direttamente dal 4G al 5G autonomo e stanno aspettando che venga stabilita la copertura 5G mentre gli operatori continuano a recuperare gli investimenti in 4G, poiché la distribuzione in 5G richiede molti investimenti nei costi di infrastruttura. Così EPRS | European Parliamentary Research Service, in "2020: l'inizio dell'era del 5G. Una gara mondiale per lanciare il 5G - "*Ten issues to watch*", gennaio 2020.

cittadini/utenti e del mercato grazie non solo al "*Network Slicing*"[143], proprietà specifica della tecnologia 5G che consente di realizzare più reti virtuali con caratteristiche diverse su un'unica infrastruttura fisica, ma anche all'uso dell'intelligenza artificiale che permetterà di analizzare e interpretare i dati in modo veloce e preciso[144].

3.2. I profili di sicurezza

Questa la ragione perché le sue vulnerabilità potrebbero essere sfruttate per compromettere sistemi e infrastrutture vitali, con il rischio di danni devastanti, spionaggio o furti di dati su vasta scala. Questo è tanto più preoccupante se si considera che gli stessi processi democratici, così come le consultazioni elettorali, sono basati sempre più sulle infrastrutture digitali.

Pertanto garantire la cybersicurezza delle reti 5G è questione di importanza strategica per l'Unione europea, in una fase in cui gli attacchi informatici sono sempre più numerosi e sofisticati. Date la natura interconnessa e transnazionale delle infrastrutture che sono alla base dell'ecosistema digitale e il carattere transfrontaliero delle minacce, eventuali vulnerabilità o incidenti riguardanti le reti 5G che si verificano in uno Stato membro sono destinate a incidere sull'Unione nel suo complesso.

Sono in gioco, insomma, oltre alla sicurezza di sistemi e apparati tecnologici, la stessa sovranità europea a cui sono strettamente collegati – prosegue la Commissione - con espressione enfatica ma rivelatrice della sua sensibilità al

[143] Il *Network slicing* permettte di configurare, in completa automazione, le risorse ed i parametri di rete. In tal modo su un'unica infrastruttura di rete vengono create porzioni di reti virtualizzate (*slice*), specializzabili per singolo servizio (Smart cities, industry 4.0, *public safety*, ecc) che richiedono diverse prestazioni di rete.

[144] L'automazione porterà miglioramenti in termini di efficienza dei costi e funzionalità: i droni connessi riducono la necessità di sorveglianza umana e svolgono compiti molto più velocemente e in modo più sicuro rispetto alle persone, mentre raccolgono dati a un costo inferiore e li inviano automaticamente al *Cloud* per essere analizzati e visualizzati quasi in tempo reale. Inoltre, il 5G può migliorare la qualità della connettività e delle informazioni disponibili per affrontare le calamità in siti di infrastrutture critiche ed eventi affollati. Il progetto 5Guards lo ha dimostrato dimostrando la priorità del traffico di rete attraverso sezioni diverse sulla stessa rete. Per quanto riguarda il modello di business del 5G, finora, la risposta degli operatori si è concentrata principalmente sulla riduzione dei costi e sull'aumento del numero di offerte aggregate. Tuttavia, le società di telecomunicazioni rischiano di perdere quote di mercato per diventare semplici fornitori di servizi di rete o di connettività. Al contrario, potrebbero assumere un ruolo più rilevante mediante una piattaforma centralizzata, che potrebbe anche essere gestita da chi possiede risorse complementari, come le Big Tech che dispongono di una posizione finanziaria più robusta e un'ampia base clienti. In tal senso un'eventuale partnership sarà di fondamentale importanza all'interno di ecosistemi decentralizzati. Negli Stati Uniti Verizon ha avviato un servizio di accesso wireless fisso nell'ottobre 2018 in quattro città degli Stati Uniti sulla base di uno standard proprietario. AT&T ha anche avviato un servizio mobile 5G basato sullo standard 3GPP a dicembre 2019. Il servizio è stato limitato ai clienti "friendly" (dipendenti dell'operatore di telefonia mobile o persone che utilizzano il servizio gratuitamente in cambio di rapporti sul servizio) fino al primo trimestre del 2019 ed è stato esteso ad altre città durante il primo trimestre del 2019. Verizon ha anche avviato un servizio mobile a Chicago e Minneapolis ad aprile 2019. Così Policy Brief 33, Three main regulatory challenges for 5G roll-out in Belgium, *Pol Camps, Simon Delaere and Jaco van der Bank, 7* gennaio 2020.

riguardo, quegli stessi "*valori di apertura e tolleranza*" che fanno parte del patrimonio culturale del vecchio continente. In tal senso la sicurezza delle reti 5G è essenziale per assicurare l'autonomia strategica dell'UE, come riconosciuto nella Comunicazione congiunta "*UE-Cina – Una prospettiva strategica*" del 12 marzo 2019[145].

Sicurezza nazionale, sovranità, autonomia strategica europea: sono infatti questi i concetti da qualche tempo al centro dello sforzo dispiegato da Stati nazionali e istituzioni europee.

In concreto, si tratta di approntare adeguati strumenti di difesa rispetto all'aggressiva strategia posta in essere dal governo cinese e dalle sue principali imprese, Huawei e ZTE, sempre più presenti nel mercato europeo e con un ruolo crescente nello sviluppo della tecnologia e nel dispiegamento delle reti 5G. Tali due società (la seconda di proprietà statale) sono sospettate dagli Stati Uniti di costituire un potenziale veicolo di spionaggio (insieme a Hytera Communications Corporation, Hangzhou Hikvision, e Dahua Technology). Fra queste Huawei, che nel 2018 ha superato Apple come secondo maggior produttore di *smartphones* al mondo dopo Samsung, è attualmente l'unica società in grado di produrre tutti gli elementi di una rete 5G (i suoi concorrenti, Nokia ed Ericsson, si stanno impegnando per offrire una valida alternativa).

E' del 19 marzo 2019 il rapporto "*Huawei, 5G, and China as a Security Threat*", elaborato dal *Nato Cooperative Cyber Defence Centre of Excellence* (CCDCOE) che evidenzia i fattori che hanno consentito a Huawei di affermarsi quale società leader: la politica nazionale cinese di superiorità tecnologica e il quadro giuridico di riferimento. Il rapporto rileva come le reti 5G siano destinate a costituire il sistema nervoso digitale delle società contemporanee ed evidenzia le delicate implicazioni strategiche insite nella scelta, da parte di paesi e imprese europee, di privilegiare l'interlocutore cinese, considerata l'aggressiva strategia di politica industriale di quel governo messa in atto anche mediante lo strumento della partnership pubblico-privata. Il rapporto indica che la rete può essere utilizzata anche per le comunicazioni critiche e, a prescindere dalle vulnerabilità tecnologiche, la scelta di affidarsi alla tecnologia fornita da un solo fornitore può creare un vincolo difficilmente rescindibile, in grado di compromettere l'autonomia di un paese e la sua stessa sovranità digitale.

Il quadro normativo cinese peraltro, è piuttosto articolato: oltre alla legge sull'*intelligence* nazionale del 2016, comprende quelle in materia di controspionaggio (2014), sicurezza dello Stato (2015), anti-terrorismo (2015), nonché la legge sulla gestione delle organizzazioni non governative straniere (2016) e quella sulla sicurezza informatica (2016).

La legge sull'*intelligence* richiede in particolare che i cittadini e le società cinesi collaborino con i servizi di sicurezza statale per raccogliere informazioni senza

[145] Comunicazione congiunta al Parlamento europeo, al Consiglio europeo e al Consiglio UE-Cina – Una prospettiva strategica, del 12 marzo 2019 JOIN(2019) 5 final

rivelare tale collaborazione. Il testo è chiaro al riguardo: "*qualsiasi organizzazione e cittadino, in conformità alla legge, sostiene, fornisce assistenza, collabora con il lavoro dell'intelligence nazionale e mantiene il segreto su qualsiasi operazione dell'intelligence nazionale di cui sia a conoscenza*". Si tratta della legge in base alla quale la società Apple nel 2017 è stata costretta a rimuovere dal suo *store* cinese tutte le applicazioni che consentivano agli utenti di bypassare il "*Great Firewall*".

Il MIT (*Massachussett Institute of Technology*) ha rescisso ogni legame con i gruppi Huawei e ZTE avviando una verifica di tutte le ricerche scientifiche e le proposte di collaborazione con la Cina, incluso Hong Kong. Ha altresì dichiarato di non volersi impegnare in futuri progetti di ricerca con tali due imprese né di rinnovare quelli esistenti. Il processo di revisione avviato dal MIT riguarda peraltro anche Russia e Arabia Saudita, oltre alla Cina. Le preoccupazioni sono rivolte ai profili inerenti la proprietà intellettuale, i controlli all'esportazione, la sicurezza e l'accesso ai dati, ma si allargano fino a comprendere la competitività economica e la sicurezza nazionale, financo i diritti politici, civili e umani. Diverse università negli Stati Uniti e nel Regno Unito, incluse Stanford e Oxford, hanno già bloccato ogni finanziamento proveniente da Huawei dopo che il governo USA ha accusato il gruppo di aver sottratto tecnologia e disatteso le sanzioni contro l'Iran.

L'atteggiamento assunto dagli Stati nei confronti della tecnologia cinese è alquanto vario.

Si passa dagli strumenti normativi o amministrativi vincolanti rivolti a specifici produttori, come nel caso di Stati Uniti e Repubblica Ceca, alle linee guida dell'Estonia. Australia e Giappone hanno adottato direttive obbligatorie in tema di sicurezza che escludono i fornitori potenzialmente controllati da governi stranieri. La Nuova Zelanda ha bloccato il piano di un operatore di distribuire la tecnologia 5G di Huawei in base alla legge sulle telecomunicazioni del 2013 a causa di "*rischi significativi per la sicurezza nazionale*".

Gli Stati Uniti nel 2018 hanno adottato una legge che vieta l'acquisto e l'uso di prodotti di telecomunicazioni e sorveglianza di specifiche società cinesi.

Diversi paesi invece hanno scelto di astenersi dall'introdurre divieti. Il primo ministro slovacco ha rilevato che non considera Huawei una minaccia per la sicurezza e che occorrono prove per imporre restrizioni. In senso analogo, il capo dell'Ufficio federale per la sicurezza delle informazioni (BSI) della Germania ha rilevato, nell'ottobre 2018, che sarebbero state necessarie prove per vietare gli apparati cinesi. Tale posizione è stata, tuttavia, rivista nel febbraio 2019, allorché è emerso l'orientamento di consentire a Huawei di partecipare alla messa in opera della rete 5G già programmata, a condizione che Pechino fornisca adeguate garanzie sulla sicurezza dei dati tramite un accordo simile a quello intercorso con gli Stati Uniti nel 2015. Pare insomma che la Germania intenda perseguire una sorta di terza via fra l'esclusione *tout court* decisa da alcuni paesi e la creazione di un sistema di sicurezza come quello messo a punto nel Regno Unito.

Qui opera dal 2010, creato dal governo, un centro di valutazione della sicurezza informatica di Huawei (HCSEC), con una commissione di supervisione controllata dall'autorità per la sicurezza informatica NCSC e incaricata di riferire al GCHQ (l'autorità per l'intelligence e la sicurezza del Regno Unito) che, anche per le sue modalità di funzionamento, può essere considerato una *best practice* (organismi simili sono stati di recente istituiti in Germania e Belgio). L'HCSEC ha evidenziato una serie di problemi e vulnerabilità che potrebbero essere sfruttate a fini illeciti.

Il gruppo BT, principale operatore di telecomunicazioni del Regno Unito, ha annunciato nel dicembre 2018 la decisione di abbandonare i dispositivi Huawei (sia i 3G e i 4 G in uso sia il 5G); Deutsche Telekom sta rivedendo la propria strategia di vendita nei confronti della società cinese, mentre Orange (ex France Telecom) ha annunciato che non avrebbe più usato i suoi dispositivi.

Peraltro il 23 aprile 2019 il Consiglio per la sicurezza nazionale ha deciso di consentire a Huawei di fornire parte dell'infrastruttura. Il giorno dopo tale decisione è stata al centro della discussione alla conferenza di Glasgow sulla cybersicurezza, che per due giorni ha riunito i vertici di organismi governativi, agenzie di sicurezza e industria dei paesi del "*Five Eyes*" (Stati Uniti, Gran Bretagna, Australia, Nuova Zelanda e Canada).

Il consesso, aperto dal Segretario britannico agli esteri, era dedicato a come rendere "*libero, aperto, pacifico e sicuro*" il cyberspazio ma - come era facilmente prevedibile - si è per lo più concentrato sulla scelta britannica che, a dispetto dei moniti statunitensi, ha rotto il fronte guidato dall'Australia che ha escluso *tout court* la società cinese da ogni fornitura inerente la rete mobile di quinta generazione.

Gli inglesi hanno precisato che la società cinese sarà comunque esclusa dal "cuore" del sistema, vale a dire gli elementi più sensibili. Tuttavia ciò non attenua la portata di una decisione controversa, risultato di un dibattito durato mesi, che si inserisce in una fase di crescente competizione economica, politica e militare fra Cina e paesi occidentali.

Come rilevato, si ritiene infatti che gli apparati cinesi possano facilitare azioni di spionaggio o sabotaggio, con il rischio di mettere in pericolo il flusso di dati sensibili fra Stati Uniti ed Europa e non consentire più il consueto scambio di informazioni fra i servizi di *intelligence*. I cinesi sostengono, al contrario, che all'esito di verifiche accurate non sia emerso alcun elemento critico, la loro tecnologia sia più conveniente e rapidamente disponibile, farne a meno rischierebbe di ritardare l'introduzione di una tecnologia altamente innovativa con un aggravio di costi per le casse del Regno Unito pari a circa 7 miliardi di sterline.

Il National Cyber Security Centre (NCSC) britannico, il braccio armato in tema di cybersicurezza del GCHQ, l'autorità per l'intelligence e la sicurezza, verifica da circa dieci anni gli apparati e i codici di Huawei presso il citato Huawei Cyber Security Evaluation Centre (HCSEC). Tale centro, con base nell'Oxfordshire, è stato creato nel 2010 come condizione perché Huawei potesse essere coinvolta come fornitore nelle infrastrutture di telecomunicazioni.

Nel marzo 2019 l'HCSEC ha dichiarato di non poter escludere la possibilità di rischi a lungo termine per la sicurezza nazionale derivanti dal coinvolgimento di Huawei nelle reti critiche del Regno Unito tuttavia, considerate le informazioni di cui dispone, ha rilevato di essere in grado di gestirli. È probabile che sia stato questo elemento a indurre il governo a decidere di scartare l'ipotesi di disporre un totale divieto.

Il governo britannico ha dichiarato il 28 gennaio 2020 che consentirà avrebbe consentito a Huawei di sviluppare parte delle proprie reti di prossima generazione. Considerato un fornitore ad alto rischio, la partecipazione di Huawei alla rete sarà comunque limitata al 35 per cento della rete ed esclusa dalle infrastrutture più strategicamente sensibili, come l'energia nucleare e i sistemi di difesa.

Peraltro, come segnalato lo scorso anno dal capo dei servizi di sicurezza australiani (ASD – *Australian Signals Directorate*), dal punto di vista tecnico la distinzione tra elementi centrali ("*core*") e secondari ("*edge*") del sistema non è del tutto chiara per le reti 5G. Il che significa che la potenziale minaccia che riguarda un punto specifico della rete la metterebbe in pericolo per intero. Di qui la decisione dell'Australia di escludere *tout court* Huawei dal 5G. Sulla stessa linea Robert Strayer del Dipartimento di Stato USA, che ad aprile ha dichiarato che dal punto di vista tecnico la distinzione fra centro e periferia di una rete 5G non è rilevante proprio a causa della sua "bassa latenza" (tempi di risposta rapidi), con una attività di elaborazione che avviene più ai suoi margini che al centro.

Il nostro paese ha esteso al 5G l'ombrello protettivo del cosiddetto *Golden Power* (tema sul quale ci si sofferma nel paragrafo 3.4) disciplinato dalla legge n. 56/2012, affidando al governo il compito si svolgere una specifica una valutazione al riguardo. L'art. 1 bis del decreto legge n. 22/2019 qualifica infatti tutti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, da chiunque forniti, come "*attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale*" abilitando il governo a fare uso dei poteri previsti per fronteggiare i rischi di un uso improprio dei dati "*con implicazioni sulla sicurezza nazionale*".

Peraltro, come rileva Bruce Schneier (*Harvard Kennedy School*) in *Foreign Policy* del 10 gennaio 2020, escludere dall'infrastruttura aziende che non offrono adeguate garanzie di sicurezza non è di per sé sufficiente a garantire sicurezza al 5G, né lo è vietare microchip, software o programmatori cinesi. Le vulnerabilità di sicurezza negli standard, nei protocolli e nel software per il 5G permangono indipendentemente da chi fornisce l'hardware e il software, risultato di scelte di mercato che ancor oggi privilegiano i costi rispetto alla sicurezza. Schneider sostiene che se gli Stati Uniti sono seriamente intenzionati a contrastare le minacce alla sicurezza nazionale legate alla rete 5G devono attribuire maggiore importanza alla sicurezza della rete rispetto all'obiettivo, pur legittimo, delle società il proprio profitto, così come a quello di perseguire i profitti aziendali e allo stesso spionaggio del governo. A dire il vero, ci sono significativi miglioramenti della sicurezza del 5G rispetto al 4G: crittografia, autenticazione, protezione dell'integrità, privacy e disponibilità della rete. Ma è la stessa configurazione della rete ad aumentare la sua

vulnerabilità agli attacchi ed essendo il 5G un'evoluzione del 4G gli aggressori potrebbero essere in grado di forzare i sistemi 5G utilizzando i protocolli 4G più vulnerabili. Inoltre vi è, come rilevato, un problema di standard: molte delle nuove funzionalità di sicurezza del 5G sono facoltative e gli operatori di rete possono scegliere di non metterle in atto, come avvenuto con il 4G. Allora diversi operatori avevano ignorato alcune delle funzionalità di sicurezza previste come obbligatorie in quanto costose. Nel novembre 2019 sono state evidenziate vulnerabilità che consentono agli utenti di 5G di essere rintracciati in tempo reale, ricevere falsi allarmi o di essere disconnessi dalla rete. Cinesi, iraniani, nordcoreani e russi hanno fatto irruzione nelle reti USA per anni pur controllare risorse di hardware, software o società produttrici di dispositivi. Nulla impedisce che con il 5G tutto ciò non continui o addirittura si accentui in futuro. Gli Stati Uniti – sottolinea Schneider - hanno bisogno di una politica nazionale che dia priorità alla sicurezza rispetto ai profitti delle aziende e alla stessa sorveglianza posta in essere dalle agenzie governative. La geopolitica del 5G peraltro è complessa e non riguarda solo la sicurezza. Il governo cinese sta sovvenzionando l'acquisto degli apparati di rete da parte delle sue società nei paesi di tutto il mondo, la tecnologia diventerà rapidamente un'infrastruttura critica nazionale ed i problemi di sicurezza avranno un'importanza crescente. Il che significa che gli attacchi criminali e le operazioni cyber da parte dei governi diventeranno la norma, purtroppo. Alla fine, conclude lo studioso, Washington dovrà intervenire con decisione e l'auspicio è che non sia troppo tardi.

Dal punto di vista strategico, la contesa con la Cina, che ha nel 5G il suo punto focale, è stata qualificata nei termini di un vero e proprio "scontro di civiltà" dal Dipartimento di Stato USA (così J. Gehrke sul *Washington Examiner* il 30 aprile 2019). Si tratta in effetti di una competizione con una civiltà e un'ideologia molto diversa da quella con la quale sinora gli Stati Uniti si sono confrontati. Il regime di Pechino, a differenza del regime sovietico (e delle stesse teorie marxiste), non è figlio della filosofia e della cultura occidentale. Di qui la necessità di ridefinire la strategia di sicurezza nazionale considerando che Russia e Cina che non sono equivalenti, in quanto quest'ultima rappresenta un concorrente non solo sul piano economico ma anche ideologico e la contesa in corso è molto diversa dalla quella che ha guidato la strategia americana di contenimento dell'Unione sovietica durante la guerra fredda.

3.3. Dimensione strategica e ruolo dell'Unione europea

L'*European Council on Foreign Relations* dedica il rapporto di giugno 2019 al ruolo dell'Unione europea e alla sua "*sovranità strategica*". Ci si interroga su come "*come l'Europa* [possa] *riacquistare la capacità di reagire*", cercando di analizzare le ragioni della crescente vulnerabilità degli Stati europei alle pressioni di paesi come la Cina, che ne mettono a rischio sicurezza, benessere economico e libertà di azione.

L'incapacità di comprendere e affrontare in modo adeguato le sfide globali poste dalla stretta correlazione fra sicurezza e questioni economiche è tale da pregiudicare la stessa indipendenza degli Stati europei. Pur mantenendo il sostegno

ad un ordine complessivo basato sulla "*rule of law*" e sull'alleanza transatlantica, l'Europa dovrebbe – questa la tesi di fondo del documento – elaborare una propria "sovranità strategica", oltre ad un adeguato sistema di *governance*, strumento essenziale per ritrovare un'identità, essenziale per esercitare potere sul piano geopolitico.

In una competizione in cui la Russia usa come armi forniture energetiche, capacità cyber e disinformazione, la Cina si serve degli investimenti finanziari quale strumento strategico, con un capitalismo di Stato con il quale forgia il mercato, la Turchia strumentalizza il flusso migratorio e l'Arabia Saudita fa leva sulle risorse energetiche, emerge un dato di cui l'Europa sembra non tener conto, vale a dire la stretta connessione fra obiettivi economici e tecnologici, sicurezza e concorrenza globale. A dispetto della circostanza che l'Unione europea nel suo complesso disponga di rilevante potere di mercato, consistente capacità di spese militari e peso diplomatico, la sua scarsa rilevanza sul piano internazionale rischia di pregiudicare gli stessi paesi membri, con la conseguenza di diventare la semplice scacchiera in cui sono altri a giocare.

Ne è dimostrazione il caso dell'intelligenza artificiale (IA), destinata a rivoluzionare non solo la tecnologia ma la stessa società, la cui rilevanza dal punto di vista strategico pare essere stata solo di recente compresa dall'UE e dalla maggior parte dei suoi membri, a differenza di Stati Uniti, Russia e Cina, paesi che hanno da tempo adottato programmi di sviluppo tecnologico focalizzati sull'interesse nazionale, potenziando l'azione dei propri governi a protezione dei propri campioni e per l'accesso ai Big Data che alimentano l'IA.

Questo comporta la necessità di riallineare obiettivi e strumenti di un'integrazione europea che deve ormai cambiare passo. La difesa e la sicurezza erano stati concepiti per demilitarizzare l'Europa piuttosto che per dotarla di una reale capacità d'azione, la politica di concorrenza serviva *in primis* per combattere aiuti di Stato e comportamenti abusivi piuttosto che difendere consumatori e imprese dai pericoli esterni. Lo stesso per le politiche di ricerca, più orientate a distribuire risorse che a perseguire i migliori risultati nella contesa tecnologica globale.

Ecco perché oggi la sfida principale per l'UE è piuttosto di aggiornare e ridefinire il proprio quadro giuridico per consentire agli Stati membri di competere, dotarsi di un *governance* che valorizzi le competenze nazionali per costruire una sovranità europea basata su quella dei singoli paesi, come teorizzato dallo storico inglese Alan Milward, che abbia fra i suoi obiettivi e presupposti lo sviluppo tecnologico. In concreto questo significa, per l'IA, far leva sul suo già collaudato ed efficace assetto regolamentare per sviluppare banche dati adatte alla ricerca mentre, per la difesa e la sicurezza, disporre di un servizio investigativo che si occupi delle interferenze straniere (la minaccia "ibrida") e, sul piano geopolitico, affinare la capacità di risposta a Est confermando il proprio impegno per la sicurezza regionale, in sintonia con l'alleanza transatlantica e gli sforzi NATO.

Al riguardo la risposta più convincente è stata quella sul piano regolamentare, in particolare con due interventi normativi, a distanza di pochi giorni l'uno dall'altro. Si

tratta *in primis* del regolamento 2019/452 del 19 marzo 2019 entrato in vigore il 10 aprile (su cui ci si sofferma al par. 3.7), che istituisce un sistema di controllo degli investimenti diretti esteri in Europa, in aree e attività strategiche**,** per proteggere sicurezza e ordine pubblico. A ciò si aggiunge la raccomandazione del 26 marzo, che affronta il tema della sicurezza delle reti di quinta generazione. Integra tale quadro normativo anche il codice europeo delle comunicazioni elettroniche, di cui alla direttiva 1972 del 2018[146], il cui termine di trasposizione scade il 21 dicembre 2020. Il suo Titolo V (gli articoli 40 e 41) è dedicato alla sicurezza, con poteri rilevanti affidati alle autorità competenti che al riguardo avranno la possibilità di impartire agli operatori istruzioni vincolanti e attivare in taluni casi un raccordo con i gruppi di intervento per la sicurezza informatica («CSIRT») ai sensi della direttiva NIS.

Certo, sono pur sempre gli Stati membri ad essere responsabili della sicurezza nazionale (lo stabilisce con chiarezza l'articolo 4, par. 2, TEU e ne fa cenno il considerato 16 del regolamento 2016/679), ma l'Unione europea ritiene, a ragione, di dover dispiegare un intervento sui profili di cybersicurezza, a protezione di reti, sistemi e dati a tutela dello stesso mercato interno. Ciò in considerazione del carattere sovranazionale delle minacce e della circostanza che dispone di strumenti, strutture e risorse che le consentono di agire con più efficacia rispetto ai singoli Stati per proteggere un sistema di scambi ormai basato sul digitale e sul commercio elettronico. Dunque, è la natura interconnessa delle infrastrutture digitali a giustificare un'azione volta a fornire incentivi e sostegno agli Stati membri perché sviluppino e mantengano capacità nazionali di cibersicurezza in stretto raccordo fra loro e con le istituzioni europee. Di qui la necessità di una strategia integrata, a livello nazionale ed europeo, con un approccio basato sulla valutazione dei rischi piuttosto che su misure di mitigazione successive.

Ancorché non ne sia mai fatta menzione, sono soprattutto la Cina e l'aggressiva strategia delle sue arrembanti imprese al centro dell'attenzione dell'UE. Gli stessi capi di Stato e di governo UE nel Consiglio del 22 marzo 2019 avevano sollecitato la Commissione europea ad agire con un "*approccio concertato*" in materia di sicurezza delle reti 5G, necessario per salvaguardare la già citata '"autonomia strategica"dell'Unione, obiettivo individuato nella stessa comunicazione congiunta "*EU-China, a Strategic Outlook*" del 12 marzo dello stesso anno.

3.4. Gli Stati Uniti e la *Black List*

Il 16 maggio 2019 il Dipartimento del Commercio USA ha inserito Huawei in una "*black-entity list*", introducendo il divieto per le compagnie americane di fare affari con il colosso di Shenzen.

Non si tratta di un fulmine a ciel sereno. I segnali, forti e chiari, erano da tempo visibili, a imprese e paesi, nell'ambito di una strategia ad ampio raggio avviata dal Dipartimento di Stato e da quello del Commercio USA a tutela della sicurezza nazionale. Nel mirino, la Cina e le società cinesi, Huawei in particolare, il maggiore

[146] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche, in GU L 321/36 del 17 dicembre 2018.

fornitore di apparati di telecomunicazioni che nel 2018 ha superato Apple come secondo produttore di *smartphones* al mondo dopo Samsung.

A gennaio dello stesso anno il Dipartimento di Giustizia USA aveva contestato a Huawei 23 reati, relativi a furto di proprietà intellettuale, ostruzione della giustizia e frodi legate all'inosservanza delle sanzioni contro l'Iran. Ma già dal 2012 gli Stati Uniti avevano vietato alle proprie aziende di utilizzare apparecchiature di rete Huawei, società che in seguito all'inserimento nella "*Security Entity List*" è stata esclusa da tutte le reti di comunicazione. Nel frattempo, una legge del 2018 aveva vietato l'acquisto e l'uso di prodotti di telecomunicazioni e sorveglianza di una serie di società cinesi. Nel mirino, insieme a Hytera Communications Corporation, Hangzhou Hikvision, e Dahua Technology, soprattutto ZTE (di proprietà statale) e Huawei, sospettate di costituire un potenziale veicolo di spionaggio.

Ma se gli investimenti in infrastrutture costituiscono la cifra distintiva dell'espansionismo cinese, non c'è solo il 5G e le telecomunicazioni ad essere al centro dell'interesse di Pechino. Giova ricordare che (come rilevato al par. 1.3.5.) nel delicato settore dei cavi sottomarini, Huawei è da tempo presente sia come fornitore attraverso Huawei Marine, sia come acquirente diretto in consorzio con altre società[147].

Non si tratta pertanto di fronteggiare soltanto i rischi per la sicurezza di reti e sistemi o per la raccolta e il trasferimento indebito di informazioni critiche, ma anche di rafforzare gli strumenti di controllo degli investimenti e delle esportazioni mediante una verifica di sicurezza nazionale. Così è avvenuto negli Stati Uniti nel 2018, allorché è stata aggiornata la legislazione sul controllo delle esportazioni e degli investimenti con l'*Export Control Reform Act* (ECRA) e l'*External Investment Risk Review Modernization Act* (FIRRMA), divenuti legge il 13 agosto dello stesso anno. Nel 2018 il governo del Regno Unito ha annunciato l'intenzione di prevedere una siffatta verifica per le fusioni e gli investimenti esteri suscettibili di creare rischi per la sicurezza nazionale, con la possibilità di bloccarli o sospenderli. Lo stesso è avvenuto in Germania.

3.5. Il regolamento europeo UE 2019/452

Nel luglio del 2016 i governanti europei sono stati colti di sorpresa dall'acquisto della società tedesca di robotica KUKA da parte della cinese Midea. L'UE aveva finanziato la fase iniziale di attività dell'azienda ed era preoccupata per l'acquisizione da parte della Cina di una tecnologia sensibile che l'UE aveva contribuito a sviluppare. Di qui il segnale che fosse giunto il momento di adottare un qualche strumento di salvaguardia per le imprese europee. Occorreva introdurre un meccanismo per verificare gli investimenti esteri e proteggere progetti o programmi di interesse dell'Unione, come quelli nei settori di ricerca, spazio, trasporti, energia e telecomunicazioni.

[147] Si tratta di una *joint venture* (anch'essa presente nella *Black List* in cui è stata da poco inserita Huawei Italia) creata nel 2008 tra Huawei (51%) e una controllata della britannica Global Marine Systems (49 %), attiva in tutto il mondo e che, come altri attori cinesi, partecipa a progetti di finanziamento in diversi paesi in via di sviluppo, sostenuti da China ExIm Bank.

In tale contesto nasce il regolamento europeo 452 del 19 marzo 2019[148], entrato in vigore l'8 aprile 2019 e applicabile a partire dall'11 ottobre 2020, tassello essenziale della strategia dell'UE. Prevede un sistema di controllo degli investimenti diretti esteri in Europa nei beni, nelle tecnologie e nelle infrastrutture critiche, al fine di proteggere sicurezza e ordine pubblico.

Si tratta di una serie di regole per il monitoraggio e la cooperazione tra Stati membri e Commissione europea che hanno ad oggetto la condivisione delle informazioni, la notifica di alcune fattispecie, la elaborazione di pareri e requisiti minimi per i meccanismi nazionali di verifica. Obiettivo del regolamento è creare un quadro procedurale di coordinamento per gli Stati che già dispongono di un meccanismo di controllo o che intendono adottarne uno e assicurare che tale meccanismo soddisfi alcuni requisiti (indicati dall'art. 3, quali la possibilità di ricorso contro la decisione, il principio di non discriminazione, ecc.).

Riguarda in sostanza gli investimenti esteri diretti (di seguito IED) provenienti da paesi terzi, ossia quegli investimenti "*che stabiliscono o mantengono legami durevoli e diretti tra investitori di paesi terzi, compresi le entità statali, e le imprese che esercitano un'attività economica in uno Stato membro*"[149]. Il regolamento si applica a tutti i settori dell'economia e non è soggetto ad alcuna soglia. La necessità di controllare un'operazione è infatti indipendente dal valore dell'operazione stessa; per esempio le *start-up* possono avere un valore relativamente limitato ma rivestire importanza strategica in settori quali la ricerca o la tecnologia.

E' previsto l'obbligo per uno Stato di notificare alla Commissione e agli altri Stati gli investimenti esteri diretti che siano oggetto di controllo fornendo una serie di informazioni (indicate all'art. 9); un altro Stato può formulare osservazioni a quello che sta effettuando la verifica se ritiene che l'investimento diretto estero possa incidere su sicurezza o ordine pubblico (art. 6, par. 1). In tal caso la Commissione europea può adottare un parere destinato allo Stato che effettua il controllo se ritiene che un investimento diretto estero possa avere incidenza su più paesi. Infine, un'acquisizione estera che possa incidere su progetti o programmi di interesse per l'Unione è soggetta a un esame più approfondito da parte della Commissione, i cui pareri devono essere presi nella massima considerazione dagli Stati membri. È quanto avverrebbe nel caso, per esempio, di investimenti esteri nelle imprese europee beneficiarie di finanziamenti a titolo di Orizon 2020, il programma di ricerca e innovazione dell'UE. Insomma, la Commissione può rivolgere allo Stato membro in cui ha luogo l'investimento pareri con i quali sono raccomandate azioni specifiche, in particolare qualora vi sia il rischio che l'investimento incida su progetti e programmi di interesse per l'Unione[150].

[148] Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019 che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione, in GU L 73 del 21 marzo 2019.

[149] Cfr. il considerando 9 del regolamento.

[150] Cfr. G. NAPOLITANO, *Il Regolamento sul controllo degli investimenti esteri diretti: alla ricerca di una sovranità europea nell'arena economica globale*, in *Rivista della regolazione dei mercati*, n. 1, 2019.

Come rilevato, si tratta di linee guida e indicazioni operative per l'esame degli investimenti esteri; lo Stato membro mantiene pertanto il potere di valutarli e decidere autonomamente, essendo responsabile della propria sicurezza nazionale, ai sensi dell'art. 4, par. 2, del trattato sull'Unione europea (TUE) e ha il diritto di proteggerla, come previsto dall'art. 346 del trattato sul funzionamento dell'Unione europea (TFUE). Il regolamento infatti fa espressamente salva la competenza esclusiva degli Stati membri in tema di sicurezza nazionale e il loro diritto di tutelare i propri interessi essenziali (art. 1).

Gli Stati membri sono dunque liberi di mantenere, modificare o adottare specifici meccanismi di controllo degli investimenti diretti esteri nel loro territorio per motivi di sicurezza o di ordine pubblico, che debbono tuttavia essere notificati alla Commissione europea (art. 3).

Nel determinare se un investimento diretto estero incida sulla sicurezza o sull'ordine pubblico, gli Stati membri e la Commissione europea possono prendere in considerazione i suoi effetti potenziali su: infrastrutture critiche, tra cui energia, trasporti, comunicazione, archiviazione dati, infrastruttura spaziali o finanziarie, infrastrutture sensibili; tecnologie critiche, tra cui intelligenza artificiale, robotica, semiconduttori, cybersicurezza, tecnologia spaziale o nucleare; sicurezza dell'approvvigionamento di fattori produttivi critici; accesso a informazioni sensibili o capacità di controllare informazioni sensibili (art. 4, par. 1). Tra i criteri da considerare ai fini di tale valutazione vi è anche la circostanza che l'investitore estero sia un soggetto controllato dal governo di un paese terzo, direttamente o indirettamente, anche attraverso l'assetto proprietario o consistenti finanziamenti, sia già stato coinvolto in attività che incidono sulla sicurezza o sull'ordine pubblico in uno Stato membro o che vi sia un serio rischio che l'investitore straniero svolga attività illegali o criminali (art. 4, par. 2).

Gli Stati membri e la Commissione possono "*tenere conto di tutti i fattori pertinenti, compresi gli effetti sulle infrastrutture critiche, sulle tecnologie, comprese le tecnologie abilitanti fondamentali, e sui fattori produttivi che sono essenziali per la sicurezza o il mantenimento dell'ordine pubblico la cui perturbazione, disfunzione, perdita o distruzione avrebbe un impatto significativo in uno Stato membro o nell'Unione*"[151]. Tra gli elementi di cui tenere conto in sede di controllo di un investimento estero, il regolamento fa esplicito riferimento ai rischi per le infrastrutture sanitarie e quelle relative alla fornitura di elementi chiave; nel mercato interno europeo i rischi posti da un investimento non si fermano necessariamente alle frontiere dello Stato membro in cui l'investimento viene effettuato.

Per questo motivo il regolamento non prevede solo la possibilità che la Commissione emetta un parere in merito a un investimento specifico: anche gli Stati membri diversi da quello in cui ha luogo l'investimento possono interloquire chiedendo informazioni e formulando osservazioni.

[151] Cfr. il considerando 13 del regolamento.

Il 25 marzo 2020 la Commissione europea ha pubblicato una comunicazione contenente orientamenti volti a coordinare l'approccio dell'UE al controllo degli investimenti[152] alla luce della crisi COVID-19 e proteggere le risorse e le tecnologie critiche dell'UE da potenziali acquisizioni e investimenti ostili da parte di società non UE[153].

In tali linee guida, la Commissione osserva che "*Nel contesto dell'emergenza da COVID-19, potrebbe aggravarsi il rischio che si verifichino tentativi di acquisizione, tramite investimenti diretti esteri, di aziende della filiera dell'assistenza sanitaria (ad esempio per la fabbricazione di dispositivi medici o di protezione) o di settori correlati, quale quello degli istituti di ricerca (ad esempio per lo sviluppo di vaccini). Occorre vigilare per garantire che gli IED non abbiano effetti negativi sulla capacità dell'UE di soddisfare le esigenze sanitarie dei suoi cittadini*".

In generale, le Linee guida cercano, almeno in parte, di anticipare l'applicazione del Regolamento 2019/452 evidenziando il suo campo di applicazione e illustrando il ruolo dello screening degli IDE in caso di emergenza sanitaria pubblica.

A tal fine la Commissione europea invita gli Stati membri ad avvalersi appieno, sin da ora, dei meccanismi di controllo degli investimenti previsti dal regolamento (operativo dall'11 ottobre 2020) per tenere conto dei rischi per le infrastrutture sanitarie critiche e per l'approvvigionamento di materiali. Raccomanda altresì di istituire un siffatto sistema a quegli Stati membri che attualmente non ne dispongono avvalendosi, nel frattempo, di tutti gli altri meccanismi disponibili. Ciò per far fronte ai casi in cui l'acquisizione o il controllo di una determinata impresa, infrastruttura o tecnologia comporti un rischio per la sicurezza o l'ordine pubblico nell'UE.

Si tratta infatti di scongiurare il rischio che l'attuale crisi sanitaria comporti la vendita di *asset* preziosi da parte degli operatori industriali e commerciali europei, comprese le PMI, ad un prezzo inferiore a quello reale. Nella comunicazione la Commissione ricorda agli Stati membri le interdipendenze esistenti in un mercato integrato come quello europeo e li invita a chiedere se del caso assistenza tecnica e a coordinarsi fra loro. Meccanismi nazionali di controllo sono già peraltro in vigore in 14 Stati membri[154].

Le Linee guida evidenziano che, oltre al controllo degli investimenti, gli Stati membri possono detenere diritti speciali in talune imprese (si tratta del "*Golden power*", oggetto di uno specifico approfondimento al par. 3.8). In alcuni casi tali diritti

[152] Commissione europea, Comunicazione della Commissione, Orientamenti agli Stati membri per quanto riguarda gli investimenti esteri diretti e la libera circolazione dei capitali provenienti da paesi terzi, nonché la protezione delle attività strategiche europee, in vista dell'applicazione del regolamento (UE) 2019/452, in GU C 99 del 26 marzo 2020.

[153] Comunicazione della Commissione, *Orientamenti agli Stati membri per quanto riguarda gli investimenti esteri diretti e la libera circolazione dei capitali provenienti da paesi terzi, nonché la protezione delle attività strategiche europee, in vista dell'applicazione del regolamento* (UE) 2019/452 (2020/C 99 I/01), in GU C 99 del 26 marzo 2020.

[154] La lista è indicata in http://trade.ec.europa.eu/doclib/html/157946.htm

possono consentire allo Stato di fissare limiti a determinati tipi di investimento nelle società interessate o bloccarli. Come le altre restrizioni alla circolazione dei capitali, ai sensi dell'art. 63 TFUE (che prevede la libera circolazione dei capitali non solo all'interno dell'UE, ma anche con i paesi terzi), tuttavia esse devono essere necessarie e proporzionate al conseguimento di un legittimo obiettivo di ordine pubblico.

Nel caso di "acquisti predatori" di attività strategiche da parte di investitori esteri (per esempio volti a limitare l'approvvigionamento sul mercato UE di un determinato bene o servizio), l'eccezione più rilevante è quella relativa all'ordine pubblico o alla pubblica sicurezza di cui all'articolo 65 TFUE. Ciò potrebbe giustificare, per esempio, l'adozione di misure restrittive atte a garantire la sicurezza dell'approvvigionamento (per esempio nel settore dell'energia) o la fornitura di servizi pubblici essenziali. Questo nel caso in cui le misure meno restrittive (come quelle che impongono obblighi di servizio pubblico a tutte le società che operano in determinati settori) siano insufficienti ad affrontare in modo adeguato tale minaccia, che rischia di compromettere gli interessi fondamentali della collettività. La sanità pubblica è stata peraltro riconosciuta dalla Corte di giustizia dell'Unione europea come un motivo imperativo di interesse generale[155].

I motivi imperativi di interesse generale riconosciuti dalla Corte di giustizia in relazione ad altre libertà sancite dal trattato includono peraltro anche la protezione dei consumatori, la salvaguardia dell'equilibrio finanziario del sistema di sicurezza sociale e il conseguimento degli obiettivi di politica sociale, che potrebbero entrare in gioco in situazioni di emergenza.

Nel caso di investimenti esteri provenienti da paesi terzi in società aventi quotazioni al di sotto del loro valore reale o intrinseco, è consentito adottare restrizioni, tenendo conto dell'impatto effettivo o potenziale di tali investimenti sugli interessi pubblici coinvolti. Nella valutazione delle ragioni e della proporzionalità di tali misure, le restrizioni ai movimenti di capitali in provenienza di paesi terzi debbono valutarsi, dal punto di vista giuridico, in modo diverso rispetto alle restrizioni che riguardano i movimenti di capitali all'interno dell'UE. Il che significa che per le restrizioni applicate a operazioni che coinvolgono paesi terzi possono essere considerati ulteriori motivi di giustificazione rispetto a quelli previsti dal trattato per le operazioni intra UE.

Nel caso in cui un investimento estero abbia luogo prima dell'entrata in vigore del regolamento, vale a dire l'11 ottobre 2020, ma non sia sottoposto a un processo di verifica nazionale, il regolamento prevede che la Commissione e gli Stati membri diversi da quello in cui l'investimento viene effettuato possano fornire commenti e pareri *ex post* a partire dall'11 ottobre 2020 ed entro 15 mesi dal completamento dell'investimento estero.

Tali pareri possono portare al divieto dell'investimento da parte dello Stato membro dell'UE in cui l'investimento è stato effettuato o, in alternativa, all'adozione delle

[155] Causa C-531/06, Commissione/Italia, punto 51.

"*misure di attenuazione necessarie*" a discrezione dello Stato membro, nel rispetto della propria normativa.

La Commissione incoraggia gli Stati membri a esaminare attentamente le acquisizioni che non sono qualificabili come investimenti diretti esteri e che non rientrano nel campo di applicazione del regolamento (art. 2, par. 1) in base alle norme sulla libera circolazione dei capitali che consentono, ai sensi della giurisprudenza europea, l'applicazione di restrizioni qualora necessarie e proporzionate per raggiungere un legittimo obiettivo di ordine pubblico.

In tali casi è consentito far riferimento a motivi di "*ordine pubblico,* […] *sicurezza pubblica e* […] *salute pubblica*", tuttavia qualora tali obiettivi possano essere perseguiti con altri mezzi meno restrittivi (per esempio, misure regolamentari che impongono obblighi di servizio pubblico) allora una restrizione all'investimento straniero specifico potrebbe essere considerata sproporzionata.

Alcuni paesi dell'UE hanno modificato il proprio sistema di controllo degli investimenti esteri anche prima della pubblicazione delle linee guida della Commissione europea. Per esempio, la Spagna ha adottato misure piuttosto severe nel contesto dell'epidemia COVID-19 per proteggere la propria economia nazionale sospendendo alcune previsioni in tema di infrastrutture e tecnologie critiche per gli investitori provenienti da paesi extra UE ed EFTA. Ciò ha fatto seguito alle misure adottate in Australia, ove è stato previsto che tutti gli investimenti stranieri soggetti al *Foreign Acquisitions and Takeovers Act* 1975 siano sottoposti ad autorizzazione preventiva indipendentemente dal loro valore o dal tipo di investitore.

L'Italia ha previsto sin dal 2012 uno specifico meccanismo di controllo mediante le disposizioni in materia di poteri speciali dello Stato (il cosiddetto *Golden Power*, di cui al decreto-legge 21/2012 convertito in legge 56/2012, a cui è dedicato il cap. 3.9), previsto per i settori di difesa e sicurezza nazionale, energia, trasporti e comunicazioni. Le norme di cui all'art. 15 del decreto legge "*Liquidità*" n. 23 dell'8 aprile 2020, in corso di conversione, hanno esteso tale sistema di controllo ai settori riguardati dal regolamento europeo 452, anticipando la valutazione richiesta da quest'ultimo.

Peraltro occorre rilevare che il regolamento non è l'unico strumento previsto per controllare gli investimenti stranieri. Infatti sia la direttiva 2014/24/EU[156] in tema di appalti sia quella 2002/21/CE[157] in tema di comunicazioni elettroniche, che riguarda le reti e l'assegnazione delle frequenze (compreso il 5G), consentono agli Stati membri di adottare le misure necessarie per assicurare la protezione dei propri interessi nazionali, l'incolumità e la sicurezza pubblica. Lo stesso articolo XXI del

[156] Direttiva 2014/24/UE del Parlamento europeo e del Consiglio del 26 febbraio 2014 sugli appalti pubblici e che abroga la direttiva 2004/18/CE, in GU L 94 del 28 marzo 2014.

[157] Direttiva 2002/21/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro), in GU L 108/3 del 24 aprile 2002.

WTO/GATT[158] prevede che uno Stato parte dell'accordo possa prendere le misure più appropriate per proteggere la sicurezza dei propri interessi essenziali.

3.6 La raccomandazione sulla sicurezza del 5G

In tema di cybersicurezza delle reti 5G è la raccomandazione della Commissione europea del 26 marzo 2019[159]a fornire concrete e specifiche indicazioni, sul piano tecnico e regolamentare.

In particolare, per affrontare i rischi di cybersecurity nelle reti 5G il documento evidenzia la necessità di considerare, in primo luogo, fattori tecnici, come le vulnerabilità che possono essere sfruttate per l'accesso non autorizzato alle informazioni (cyberspionaggio, per motivi economici o politici) o per altri scopi dolosi (attacchi informatici volti a distruggere sistemi e dati o a provocarne il malfunzionamento) oppure la necessità di proteggere le reti durante il loro ciclo di vita e considerare le apparecchiature nelle fasi di progettazione, sviluppo, appalto, diffusione, funzionamento e manutenzione delle reti 5G.

Inoltre, occorre prendere in considerazione altri elementi, quali i profili di carattere strategico e regolamentare, come i requisiti normativi imposti ai fornitori di apparecchiature di comunicazione. E' necessario infatti tener conto del rischio di influenza da parte di un paese terzo in relazione al suo modello di *governance*, l'assenza di accordi di cooperazione sulla sicurezza o di una decisione di adeguatezza europea in tema di protezione dei dati, verificando altresì se il paese in questione sia parte di accordi in materia di cybersicurezza, lotta alla criminalità informatica o protezione dei dati.

Al fine di sostenere lo sviluppo di un approccio dell'Unione volto a garantire la cybersecurezza delle reti 5G, la raccomandazione in esame affida a vari soggetti istituzionali il compito di svolgere specifiche azioni al fine di consentire agli Stati membri di valutare i rischi di che interessano le reti 5G a livello nazionale e adottare le necessarie misure di sicurezza. Affida poi alle istituzioni, alle agenzie e ad altri organismi dell'Unione di elaborare congiuntamente agli Stati membri una valutazione dei rischi coordinata a livello di Unione basata sulla valutazione nazionale dei rischi. Infine, il gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 (NIS) ha il compito di individuare un'eventuale serie comune di misure da adottare per le infrastrutture che sono a base dell'ecosistema digitale, in particolare le reti 5G.

La raccomandazione prevede che entro il 30 giugno 2019 gli Stati membri svolgano una valutazione sui rischi per le reti 5G a livello nazionale e adottino le misure necessarie, compreso l'aggiornamento dei requisiti di sicurezza. Si tratta di adempimenti necessari anche ai sensi delle direttive in tema di comunicazioni elettroniche del 2002, aggiornate nel 2009, secondo cui sono le stesse reti a dover

[158] Article XXI, Security exceptions,
https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf
[159] Raccomandazione (UE) 2019/534 della Commissione del 26 marzo 2019, Cybersicurezza delle reti 5G, in GU L 88 del 29 marzo 2019.

garantire "*il mantenimento dell'integrità e della sicurezza"* e un "*livello elevato di protezione dei dati personali*" come confermato dal regolamento europeo 2016/679. Tale valutazione avrebbe poi dovuto essere trasmessa, entro il 15 luglio, alla Commissione e all'ENISA affinché gli stessi Stati, insieme alle istituzioni UE, alle agenzie e agli altri organismi potessero poi effettuare quella congiunta a livello europeo, da completarsi entro il 1° ottobre 2019 (in realtà ciò è avvenuto il 9 ottobre). La raccomandazione prevede che in seguito il Gruppo di Cooperazione, istituito ai sensi della direttiva NIS, individui entro il 31 dicembre gli strumenti atti a identificare i rischi e le possibili misure di mitigazione, tra i quali la certificazione, le prove e i controlli degli accessi.

Tale insieme di strumenti – secondo la raccomandazione - dovrebbe orientare la Commissione nello sviluppo di requisiti minimi comuni, a ulteriore garanzia di un elevato livello di cybersicurezza delle reti 5G in tutta l'Unione. Si può trattare di impegni stringenti per le imprese che partecipano alle gare per l'assegnazione dei diritti d'uso delle frequenze, specifici requisiti per le procedure di appalto così come la conformità agli schemi di certificazione di *hardware, software* o servizi.

La necessità di rispettare i rigorosi parametri e standard di resilienza, sicurezza e *compliance* previsti dalle norme e dalle certificazioni nazionali (da aggiornare e integrare costantemente per tener conto dell'evoluzione delle minacce) è infatti essenziale. Ciò dovrebbe riguardare non solo gli apparati, le piattaforme e i servizi di rete ma lo stesso processo relativo alle diverse fasi di realizzazione della rete 5, compresi i contratti già in essere relativi alle forniture e ai servizi 5G.

In tal senso hanno un ruolo fondamentale gli schemi di certificazione europei (volontari, ma destinati in futuro a divenire obbligatori) elaborati da ENISA secondo quanto previsto dal *Cybersecurity Act*[160], approvato dal Parlamento europeo il 12 marzo 2019, che costituiscono gli elementi portanti del futuro mercato continentale della cybersicurezza.

La sicurezza delle reti è destinata ad essere rafforzata altresì dalla trasposizione del codice europeo delle comunicazioni elettroniche, la direttiva 1972 del 2018[161], il cui termine scade il 21 dicembre 2020. Il suo Titolo V è dedicato alla sicurezza (articoli 40 e 41) e affida fra l'altro poteri rilevanti alle autorità competenti, che al riguardo avranno la possibilità di impartire agli operatori istruzioni vincolanti e attivare in taluni casi un raccordo con i gruppi di intervento per la sicurezza informatica («CSIRT») ai sensi della direttiva NIS. Si tratta dunque di un ulteriore, importante tassello del mosaico, da completare quanto prima, a tutela della sicurezza di reti e servizi.

3.7. La "cassetta degli attrezzi" per la sicurezza del 5G

[160] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013, in GU L 151 del 7 giugno 2019.

[161] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche in GU L 321 del 17 dicembre 2018.

Come previsto dalla raccomandazione, il gruppo di cooperazione istituito dalla direttiva NIS ha approvato il 29 gennaio scorso la "cassetta degli attrezzi" (*Toolbox*) per il 5G[162], cioè le misure di mitigazione per affrontare i rischi di sicurezza legati alle reti di quinta generazione che Stati membri dovranno applicare entro il prossimo 30 aprile.

Obiettivo è delineare un approccio europeo coordinato basato su una serie comune di misure, volte a mitigare i principali rischi di cybersicurezza delle reti 5G identificati nella relazione coordinata sulla valutazione dei rischi dell'UE del 9 ottobre 2019. Intende inoltre assistere gli Stati membri nella selezione e definizione delle priorità delle misure che dovrebbero far parte dei piani nazionali ed europei di mitigazione del rischio.

Sono gli operatori ad essere responsabili dell'attuazione sicura del 5G, ma spetta agli Stati membri la sicurezza nazionale. La sicurezza della rete tuttavia ha una rilevanza strategica che travalica i confini nazionali: riguarda il mercato unico e incide sulla stessa sovranità tecnologica dell'UE, a sua volta collegata alla competitività economica e al suo ruolo sul piano geopolitico. Dal *Toolbox* emerge che i rischi strategici non possono essere mitigati solo con misure tecniche; in questi casi occorre una risposta politica e normativa, soprattutto quando un determinato fornitore (è il caso di Huawei, peraltro mai citato nel documento) è soggetto a possibili interferenze di un governo straniero (es. la legge sulla Cybersicurezza del 2016[163]).

Pur mettendo in conto valutazioni differenziate a livello nazionale, l'obiettivo del *Toolbox* è quello di evitare che gli Stati procedano in ordine sparso. Di qui l'indicazione di un approccio metodologico comune e un armamentario condiviso. Al riguardo la Commissione si impegna a far uso di tutti gli strumenti di cui dispone per garantire la sicurezza dell'infrastruttura e dell'intera *"supply chain"* del 5G: le regole in tema di cyber sicurezza e telecomunicazioni (contenute nel Codice europeo delle comunicazioni elettroniche), il coordinamento in tema di standardizzazione e certificazione (il *Cybersecurity Act*); la verifica degli investimenti diretti esteri (il regolamento 2019/452); gli strumenti di difesa commerciale (le misure *antidumping*); le regole in tema di concorrenza e appalti pubblici; gli stessi programmi di finanziamento UE (*Connecting Europe Facility Digital*).

Con un delicato esercizio di equilibrismo, l'Unione europea cerca di mantenersi equidistante tra Stati Uniti e Cina, raccomandando alle autorità di regolamentazione nazionali di applicare le restrizioni ritenute più opportune per proteggere le parti centrali delle reti (le più vulnerabili alla pirateria informatica e allo spionaggio) e adottare misure adeguate nei confronti dei fornitori considerati "ad alto rischio".

[162] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE, Bruxelles, 29 gennaio 2020 COM(2020) 50 final.

[163] La *Cyber Security Law of the People's Republic of China*, adottata il 7 novembre 2016 ed entrata in vigore il 1° giugno 2017.

Gli Stati membri sono invitati a garantire la diversità dei fornitori e adottare una strategia "*multi-vendor*", come già avviene per il 4G. Di qui l'idea di fissare un tetto (*cap)* alla presenza di un fornitore sulla rete, come ha fatto per esempio il Regno Unito che ha annunciato quello del 35%.

Secondo il *Toolbox* tutti i fornitori "ad alto rischio" (Huawei e ZTE) dovranno essere limitati o esclusi dalle parti sensibili della rete per mitigare il rischio di interferenze statali. Non si tratta solo delle funzioni *core*, ma vi è compresa anche la rete di accesso, come già emerso nel documento di valutazione del rischio a livello UE del 9 ottobre 2019. Nel documento viene altresì confutata la distinzione tra centro e periferia (*core* ed *edge*) dei sistemi 5G, che si ritiene sia destinata ad evolvere in fretta con il passaggio dal 5G non autonomo (*non standalone*, essenzialmente un 4G potenziato ora in fase di realizzazione) al 5G autonomo. Una transizione che sposterà molti dati alla periferia della rete e aprirà la strada a una maggiore virtualizzazione delle operazioni, con un'accentuata dipendenza dall'architettura software della rete e il rischio, per esempio, che un fornitore possa introdurre vulnerabilità mediante gli aggiornamenti.

Le indicazioni della Commissione europea sono chiare: ogni Stato membro dovrebbe elaborare un piano per ridurre progressivamente la dipendenza da fornitori ad altro rischio, mentre procedono al potenziamento della loro infrastruttura. Suggerisce di prendere in considerazione esclusioni e restrizioni all'interno dei normali cicli di sostituzione degli apparati, con un periodo di transizione volto a mitigare l'impatto economico del rimpiazzo dei prodotti dei distributori cinesi.

Per ciascuna delle nove aree di rischio identificate nella relazione sulla valutazione coordinata dei rischi a livello europeo del 9 ottobre 2019, la cassetta degli attrezzi identifica e fornisce piani di mitigazione del rischio, che comprendono possibili combinazioni di misure strategiche e tecniche, insieme ad adeguate azioni di supporto per mitigare i possibili rischi.

In particolare, gli Stati membri sono invitati a rafforzare i requisiti di sicurezza per gli operatori di rete mobile (per esempio, in tema di accesso, norme sulla sicurezza del funzionamento e del monitoraggio, limitazioni sull'esternalizzazione di specifiche funzioni, ecc.). Dovrebbero altresì valutare il profilo di rischio dei fornitori e quindi applicare restrizioni mirate a quelli considerati ad alto rischio, compresa l'esclusione, qualora necessarie per mitigare i rischi per gli *asset* critici e sensibili.

Per esempio, nella procedura di aggiudicazione di un appalto la normativa vigente affida alla stazione appaltante il compito di indicare, nei documenti di gara, sia il criterio di aggiudicazione sia, nel caso dell'offerta economicamente più vantaggiosa,

gli elementi da prendere in considerazione (indicati a titolo esemplificativo al par. 6 dell'art. 95 del d.lgs. n. 50/2016[164], il codice appalti).

In tal caso è essenziale che fra tali elementi sia annoverato quello della sicurezza, soprattutto quando si tratta di beni ad alto contenuto tecnologico, come nel caso degli apparati 5G.

Al riguardo le Linee Guida n. 2 dell'ANAC (Autorità nazionale anticorruzione) relative all'offerta economicamente più vantaggiosa (approvate il 21 settembre 2016 e aggiornate il 2 maggio 2018) indicano che nella valutazione delle offerte possono essere valutati profili di carattere soggettivo qualora consentano di "*apprezzare meglio il contenuto e l'affidabilità dell'offerta o di valorizzare caratteristiche dell'offerta ritenute particolarmente meritevoli*"; in ogni caso, esse devono riguardare "*aspetti che incidono in maniera diretta sulla qualità della prestazione*".

Il che significa, per l'amministrazione, poter valutare l'adeguatezza dell'offerta tenendo conto di una pluralità di elementi (da indicare peraltro necessariamente nei documenti di gara, a garanzia della tenuta giuridica della scelta finale), compresi quelli inerenti la sicurezza della fornitura e del servizio in questione, di cui fanno parte le caratteristiche soggettive dell'eventuale contraente.

Il tema della sicurezza dei beni e dei servizi informativi è rilevante soprattutto per le forniture tecnologiche della pubblica amministrazione. Come rilevato, la sicurezza dei vari elementi destinati ad integrare i sistemi informativi della pubblica amministrazione è strettamente connessa alla verifica della qualità e dell'affidabilità degli operatori economici aggiudicatari, a tutela e garanzia dei dati e dei diritti dei cittadini oltre che della stessa sicurezza nazionale.

La stessa Commissione europea, nella raccomandazione del 26 marzo 2019, così come nel *Toolbox* in esame, ha evidenziato l'importanza di procedure di appalto che consentano la valutazione dell'adeguatezza delle offerte in base agli elementi tecnici e ai requisiti normativo-regolamentari degli operatori coinvolti nelle gare, così da verificare le caratteristiche dei singoli fornitori e non compromettere la sicurezza della "*supply chain*". La stessa valutazione coordinata del rischio dell'UE sulla sicurezza informatica di cui al rapporto del 9 ottobre 2019, evidenzia la necessità di considerare, in sede di gara, il profilo di rischio dei singoli fornitori, da valutarsi in base a fattori quali la possibilità che lo stesso sia soggetto a interferenze di un paese extra UE (pt. 2.36). Naturalmente tale valutazione dovrebbe essere condotta unicamente per motivi di sicurezza e in base a criteri oggettivi.

Peraltro la normativa vigente in tema di comunicazioni elettroniche (art. 13 bis della direttiva 2002/21) impone agli Stati membri di garantire che gli operatori di

[164] Decreto legislativo 18 aprile 2016, n. 50, Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture, in GU Serie Generale n.91 del 19-04-2016 - Suppl. Ordinario n. 10.

telecomunicazioni assicurino l'integrità delle loro reti e quindi la continuità della fornitura dei servizi. Così stabilisce anche il codice europeo delle comunicazioni elettroniche (la direttiva 2018/1972) al fine ad evitare minacce alla riservatezza, alla disponibilità e all'integrità delle risorse.

Il *Toolbox* segnala altresì la necessità che ciascun operatore disponga di una strategia *multi-vendor* per evitare o limitare la dipendenza da un unico fornitore, garantire un adeguato equilibrio dei fornitori a livello nazionale ed evitare la dipendenza dai fornitori considerati alto rischio, così da consentire l'interoperabilità delle apparecchiature.

Le misure strategiche considerate nel *Toolbox* riguardano invece il rafforzamento dei poteri regolatori delle autorità di controllo, specifiche azioni per affrontare i rischi relativi a vulnerabilità non tecniche (ad esempio il rischio di interferenza da parte di uno Stato non UE o attori sostenuti dallo Stato), per valutare il profilo di rischio dei fornitori e promuovere iniziative volte a sostenere lo sviluppo di fornitori 5G affidabili e diversificati.

La Commissione invita gli Stati membri ad adottare misure adeguate entro il 30 aprile 2020 e il gruppo di cooperazione NIS a preparare una relazione dello stato di attuazione delle misure in ogni Stato membro chiave entro il 30 giugno. Infine, entro il 10 ottobre 2020, gli Stati membri, in collaborazione con la Commissione, dovrebbero valutare gli effetti della raccomandazione della Commissione del 26 marzo 2019 ai fini di ulteriori azioni.

L'avvento del 5G mette in luce la complessa natura delle sfide tecnologiche e politiche che gli Stati membri devono affrontare e continueranno ad affrontare nei prossimi decenni. Al riguardo la Commissione europea ha dimostrato che una maggiore cooperazione in materia non è solo utile, ma necessaria per la sicurezza informatica e la sovranità tecnologica dell'Europa. La cybersicurezza è per definizione difficile da affrontare a livello nazionale ma diventa meno costosa e più efficace se il campionario delle misure o se le procedure e gli schemi di certificazione sono elaborati a Bruxelles.

Come evidenziato da Mathieu Duchâtel e François Godement nel blog dell'*Institut Montaigne* il 30 gennaio 2020, l'approccio relativo alla mitigazione del rischio, in contrapposizione all'esclusione *tout court* dei venditori ad alto rischio, implica un costante e costoso adattamento degli strumenti operativi, con una sorta di scommessa sulle future capacità della cybersicurezza europea.

A ciò si aggiunge un ulteriore, rilevante aspetto di carattere strategico, in un contesto geopolitico in cui si fronteggiano Stati Uniti e Cina: la "cassetta degli attrezzi", che consente agli Stati membri di scegliere il fornitore per le proprie reti 5G tenendo conto non solo degli elementi tecnici ma anche di quelli normativi e regolamentari, offre a questi ultimi la possibilità di rafforzare il legame con gli Stati Uniti difendendo la propria sicurezza.

3.8. Il *Golden power*

3.8.1. La disciplina normativa e il 5G. L'esempio dell'Italia

Il giorno prima dell'adozione della raccomandazione europea, il 25 marzo 2019, l'Italia ha adottato il decreto legge n. 22/2019[165], convertito in legge n. 41/2019, il cui articolo 1 bis qualifica tutti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, da chiunque forniti, come "*attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale*" abilitando il governo a fare uso dei poteri previsti dalla disciplina sul *Golden Power* per fronteggiare i rischi di un uso improprio dei dati "*con implicazioni sulla sicurezza nazionale*".

In concreto, l'impresa che stipula, a qualsiasi titolo, contratti o accordi aventi ad oggetto l'acquisizione di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti relative ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, ovvero acquisisca, a qualsiasi titolo, componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, quando posti in essere con soggetti esterni all'Unione europea, deve pertanto presentare una notifica ai sensi della normativa sul *Golden Power*.

Quella relativa al *Golden Power* è una disciplina che è stata oggetto di diverse revisioni nel corso degli anni.

Fino a qualche anno fa lo Stato aveva la possibilità di opporsi all'acquisizione di partecipazione rilevanti di qualsiasi tipo, anche intra-UE, per mezzo di apposite previsioni inserite negli statuti delle principali società di diritto italiano, ai sensi del decreto legge n. 332/1994, convertito in legge n. 474/1994, relativo alle società controllate direttamente o indirettamente dallo Stato operanti nei settori di difesa, trasporti, telecomunicazioni, fonti di energia e negli altri pubblici servizi.

Era la cosiddetta *Golden Share*, che abilitava il governo a facoltà di dettare specifiche condizioni all'acquisito di partecipazioni, porre il veto all'adozione di determinate delibere societarie e opporsi all'acquisto di partecipazioni, entrata nel mirino di Bruxelles a causa della sua contrarietà al diritto europeo. Tale normativa - come di seguito evidenziato - è stata successivamente modificata con il decreto legge 15 marzo 2012, n. 21, convertito in legge n. 56/2012, con cui il legislatore nazionale ha ridisegnato l'istituto trasformandolo in *Golden Power*.

3.8.2. Dal *Golden share* al *Golden power*

Con il decreto legge n. 21/2012 il legislatore ha recepito le censure sollevate dalla Commissione europea e aderito alle sue indicazioni, determinando il 15 febbraio 2017 l'archiviazione della procedura di infrazione da parte della Commissione europea, che ha ritenuto la nuova disciplina italiana compatibile con il Trattato sul funzionamento dell'Unione europea.

[165] Decreto-legge 25 marzo 2019, n. 22, Misure urgenti per assicurare sicurezza, stabilità finanziaria e integrità dei mercati, nonché tutela della salute e della libertà di soggiorno dei cittadini italiani e di quelli del Regno Unito, in caso di recesso di quest'ultimo dall'Unione europea, convertito con modificazioni dalla legge 20 maggio 2019, n. 41, in G.U. 24 maggio 2019, n. 120.

La disciplina relativa ai poteri speciali del Governo non riguarda solo il nostro Paese; si ricollega infatti agli istituti della *Golden Share* inglese [166] e dell'*Action spécifique* francese, che era stata oggetto di censure sollevate dalla Commissione europea[167] e di una pronuncia di condanna da parte della Corte di giustizia UE.

La Commissione europea aveva infatti rilevato che l'esercizio di tali poteri dovesse essere effettuato senza discriminazioni e ammesso qualora si fondasse su "*criteri obiettivi, stabili e resi pubblici*" e giustificato da "*motivi imperiosi di interesse generale*". In tal senso, con la legge n. 56/2012 il legislatore nazionale, anche mediante il rinvio a fonti di rango secondario[168] ha ridefinito l'istituto, in linea con quanto indicato nella comunicazione della Commissione[169] del 19 luglio 1997. Proprio tale comunicazione conteneva quegli indirizzi in base ai quali era stata avviata la procedura di infrazione nei confronti del nostro Paese e che aveva ad oggetto le disposizioni della legge n. 474/1994. Peraltro, analoghe procedure di infrazione hanno riguardato anche il Belgio, Germania, Regno Unito, Portogallo, Francia e Spagna.

3.8.3. La nuova disciplina

La disciplina di cui alla legge n. 56/2012 ridefinisce pertanto l'ambito oggettivo e soggettivo, la tipologia, le condizioni e le procedure di esercizio da parte del governo dei poteri speciali nei settori della difesa e della sicurezza nazionale, nonché di taluni ambiti di attività definiti di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.

In sostanza, il governo ha la facoltà di porre il veto rispetto all'adozione di determinate delibere, atti e operazioni delle imprese che gestiscono attività strategiche in specifici settori, di dettare impegni e condizioni in caso di acquisito di partecipazioni in tali imprese, ovvero di opporsi all'acquisto delle medesime

[166] Decreto-legge 31 maggio 1994, n. 332, recante norme per l'accelerazione delle procedure di dismissione di partecipazioni dello Stato e degli enti pubblici in società per azioni, convertito, con modificazioni, dalla legge 30 luglio 1994, n. 474: "Tra le società controllate direttamente o indirettamente dallo Stato operanti nel settore della difesa, dei trasporti, delle telecomunicazioni, delle fonti di energia, e degli altri pubblici servizi, sono individuate con decreto del Presidente del Consiglio dei ministri […], quelle nei cui statuti, prima di ogni atto che determini la perdita del controllo, deve essere introdotta con deliberazione dell'assemblea straordinaria una clausola che attribuisca al Ministro dell'economia e delle finanze la titolarità di uno o più dei seguenti poteri speciali da esercitare di intesa con il Ministro delle attività produttive […]".

[167] La disciplina della *Golden share* è stata oggetto della procedura d'infrazione n. 2009/2255, in quanto ritenuta lesiva della libertà di stabilimento e della libertà di circolazione dei capitali garantite dal trattato sul funzionamento dell'Unione europea. Nell'ambito di tale procedura di infrazione, la Commissione europea, il 24 novembre 2012, aveva deciso di deferire il governo italiano alla Corte, ex articolo 258 TFUE.

[168] Con due provvedimenti, il d.P.R. 19 febbraio 2014, n. 35, in materia di poteri speciali nei settori della difesa e della sicurezza nazionale e il d.P.R. 25 marzo 2014, n. 86 che disciplina i poteri speciali nei settori dell'energia, dei trasporti e delle comunicazioni, sono stati definiti gli ambiti soggettivi ed oggettivi di applicazione della norma primaria, così come la tipologia, le condizioni e le procedure per l'esercizio dei relativi poteri speciali.

[169] Comunicazione della Commissione relativa ad alcuni aspetti giuridici attinenti agli investimenti intracomunitari, in GU n. C 220 del 19 luglio 1997.

partecipazioni. Si tratta di un potere di intervento rilevante, che attiene alla *governance* di società operanti in settori considerati strategici e finalizzato alla tutela degli *asset* definiti di prioritaria importanza per il paese.

L'impresa che opera nei settori in questione è tenuta a notificare alla Presidenza del Consiglio dei ministri un'informativa completa circa la delibera o l'atto da adottare ai fini dell'eventuale esercizio del potere di veto, la cui proposta è affidata al Ministero dello sviluppo economico. L'inosservanza degli obblighi di notifica o l'inadempimento di impegni e condizioni derivanti dall'esercizio dei poteri sono puniti con specifiche sanzioni amministrative pecuniarie.

A differenza della precedente, la nuova disciplina estende la possibilità di esercitare i poteri speciali nei confronti di tutte le società, pubbliche o private che svolgono attività considerate di rilevanza strategica e non più soltanto rispetto alle società privatizzate o in mano pubblica (art. 1).

Alla disciplina di fonte secondaria (decreti del Presidente del Consiglio dei Ministri) è affidata la individuazione delle attività per le quali potranno essere attivati i poteri speciali, la individuazione della tipologia di atti o operazioni infragruppo esclusi dall'ambito operativo della nuova disciplina, il concreto esercizio dei poteri speciali e l'individuazione di ulteriori disposizioni attuative.

Tali poteri riguardano i settori della difesa e della sicurezza nazionale nonché taluni ambiti di attività definiti di rilevanza strategica nei settori dell'energia, dei trasporti, delle comunicazioni.

Con il d.P.R. n. 35/2014 per i settori della difesa e della sicurezza nazionale ed il d.P.R. n. 86/2014 per i settori di energia, trasporti e comunicazioni, sono stati definiti gli ambiti soggettivi ed oggettivi di applicazione della legge n. 56/2012, così come la tipologia, le condizioni e le procedure per l'esercizio dei relativi poteri speciali.

E' il d.P.C.M. 6 agosto 2014 a delineare le attività di coordinamento della Presidenza del Consiglio dei Ministri finalizzate all'esercizio dei poteri speciali, con un Gruppo di coordinamento interministeriale del quale fanno parte rappresentanti della Presidenza e componenti designati dai ministeri interessati. Il Dipartimento per il coordinamento amministrativo è l'ufficio responsabile delle attività di coordinamento, delle attività propedeutiche all'esercizio dei poteri speciali e delle relative attività istruttorie.

3.8.4. I poteri speciali nei settori di difesa e sicurezza nazionale

Come indicato, il d.P.R. 20 marzo 2014, n. 35[170] ha stabilito le procedure per l'attivazione dei poteri speciali nei settori della difesa e della sicurezza nazionale,

[170] Decreto del Presidente della Repubblica 19 febbraio 2014, n. 35, regolamento per l'individuazione delle procedure per l'attivazione dei poteri speciali nei settori della difesa e della sicurezza nazionale, a norma dell'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, in GU Serie Generale n.66 del 20 marzo 2014.

mentre con il d.P.C.M. 6 giugno 2014, n. 108[171] è stato adottato il regolamento per l'individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale. Quest'ultimo comprende le norme che individuano le attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, ivi incluse le attività strategiche chiave, di competenza sia del Ministero dell'interno sia del Ministero della difesa,.

3.8.5. I settori di energia, trasporti e comunicazioni

Così come per i settori della difesa e della sicurezza nazionale (art. 2), sono affidate alla disciplina secondaria, mediante regolamenti da adottare previo parere delle Commissioni parlamentari competenti, l'individuazione degli *asset* strategici nel settore dell'energia, dei trasporti e delle comunicazioni, l'esercizio dei poteri speciali, l'individuazione di ulteriori disposizioni attuative della nuova disciplina.

I poteri speciali relativi al settore dell'energia, dei trasporti e delle comunicazioni consistono nella possibilità di apporre il veto o specifiche condizioni da parte del governo alle delibere, agli atti e alle operazioni concernenti *asset* strategici; di porre condizioni all'efficacia dell'acquisto di partecipazioni da parte di soggetti esterni all'UE in società che detengono attivi "strategici" e, in casi eccezionali, opporsi all'acquisto stesso. Si tratta per lo più della medesima disciplina prevista dall'art. 1 in relazione alle società operanti nei settori della difesa e della sicurezza nazionale.

Gli obblighi di notifica sono estesi alle delibere, atti o operazioni aventi ad oggetto il mutamento dell'oggetto sociale, lo scioglimento della società, la modifica di clausole statutarie riguardanti l'introduzione di limiti al diritto di voto o al possesso azionario. Il veto alle delibere, atti o operazioni può essere espresso qualora essi diano luogo a una situazione eccezionale, non disciplinata dalla normativa nazionale ed europea di settore, di minaccia di grave pregiudizio per gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, ivi compresi le reti e gli impianti necessari ad assicurare l'approvvigionamento minimo e l'operatività dei servizi pubblici essenziali.

Nel computo della partecipazione rilevante ai fini dell'acquisto si tiene conto della partecipazione detenuta da terzi con cui l'acquirente ha stipulato patti parasociali. Anche per le violazioni di cui al presente articolo è prevista la sanzione della nullità degli atti.

I due regolamenti sono entrati in vigore il 7 giugno 2014. Si tratta del d.P.R. 25 marzo 2014, n. 85 [172], il regolamento per l'individuazione degli attivi di rilevanza

[171] Decreto del Presidente del Consiglio dei Ministri 6 giugno 2014, n. 108, regolamento per l'individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, a norma dell'articolo 1, comma 1, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, in GU Serie Generale n.176 del 31 luglio 2014.

[172] Decreto del Presidente della Repubblica 25 marzo 2014, n. 85, Regolamento per l'individuazione degli attivi di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, a norma dell'articolo 2, comma 1, del decreto-legge 15 marzo 2012, n. 21, in GU Serie Generale n.129 del 6 giugno 2014.

strategica" e del d.P.R. 25 marzo 2014, n. 86[173], relativo all'individuazione delle procedure per l'attivazione dei poteri speciali.

3.8.6. I settori ad alta intensità tecnologica

Con il decreto legge n. 148 del 2017[174] è stata modificata ed estesa la disciplina dell'esercizio dei poteri speciali del Governo con riferimento alla *governance* di società considerate strategiche, ampliando anche i settori ai quali i poteri speciali risultano applicabili. E' stata prevista la sanzione amministrativa pecuniaria ove siano violati gli obblighi di notifica e esteso l'esercizio dei poteri speciali applicabili nei settori dell'energia, dei trasporti e delle comunicazioni anche al settore della cosiddetta alta intensità tecnologica.

La normativa ha inoltre individuato il criterio a cui il governo deve attenersi nell'esercizio dei poteri speciali, con riferimento a quelle operazioni di acquisto da parte di soggetti extra UE di società che detengono attivi strategici nel settore energetico, dei trasporti e delle comunicazioni, ove l'acquisto di partecipazioni determini l'insediamento stabile dell'acquirente. In tali ipotesi il governo deve valutare, oltre alla minaccia di grave pregiudizio agli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, anche il pericolo per la sicurezza o per l'ordine pubblico.

3.8.7. Altri poteri speciali

Occorre rilevare che, oltre alla disciplina del *Golden Power*, altri interventi normativi hanno perseguito analoghi obiettivi di tutela delle società operanti in settori giudicati strategici per l'economia nazionale.

In particolare, sono stati previsti diritti speciali in capo all'azionista pubblico nella disciplina codicistica delle società; a ciò si aggiunge la legge 23 dicembre 2005, n. 266[175] (legge finanziaria 2006), che ha introdotto nell'ordinamento italiano la cd. *Poison pill* (pillola avvelenata) che consente, in caso di offerta pubblica di acquisto ostile riguardante società partecipate dalla mano pubblica, di deliberare un aumento di capitale, grazie al quale l'azionista pubblico potrebbe accrescere la propria quota di partecipazione vanificando il tentativo di scalata non concordata.

[173] Decreto del Presidente della Repubblica 25 marzo 2014, n. 86, Regolamento per l'individuazione delle procedure per l'attivazione dei poteri speciali nei settori dell'energia, dei trasporti e delle comunicazioni, a norma dell'articolo 2, comma 9, del decreto-legge 15 marzo 2012, n. 21, in GU Serie Generale n.129 del 6 giugno 2014.

[174] Decreto-legge 16 ottobre 2017, n. 148, Disposizioni urgenti in materia finanziaria e per esigenze indifferibili, convertito con modificazioni dalla L. 4 dicembre 2017, n. 172, in G.U. 5 dicembre 2017, n. 284.

[175] Legge 23 dicembre 2005, n. 266, Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2006), in GU Serie Generale n.302 del 29 dicembre 2005 - Suppl. Ordinario n. 211.

Con il medesimo obiettivo di salvaguardare le società d'interesse nazionale, l'articolo 7 del decreto-legge n. 34 del 2011[176] ha autorizzato la Cassa Depositi e Prestiti ad assumere partecipazioni in società di rilevante interesse nazionale. In particolare, sono state definite "*di rilevante interesse nazionale*" le società di capitali operanti nei settori della difesa, della sicurezza, delle infrastrutture, dei trasporti, delle comunicazioni, dell'energia, delle assicurazioni e dell'intermediazione finanziaria, della ricerca e dell'innovazione ad alto contenuto tecnologico e dei pubblici servizi.

3.8.8. Il caso Vivendi-TIM

Un esempio interessante di *Golden power* è quello relativo ai poteri esercitati dal governo con riferimento all'operazione di partecipazione della Società Vivendi s.a. in TIM S.p.A.

In quel caso con d.P.C.M. del 16 ottobre 2017 sono state imposte specifiche prescrizioni e condizioni nei confronti sia di Vivendi sia di Telecom Italia, comprese le due controllate Sparkle S.p.A. e Telsy Elettronica e Telecomunicazioni S.p.A., in quanto società titolari delle attività di rilevanza strategica per la difesa e la sicurezza nazionale.

Tra le prescrizioni previste alcune riguardano il mantenimento stabile sul territorio nazionale delle funzioni di gestione e sicurezza di reti, servizi e forniture che supportano attività "strategiche", altre sono volte a garantire la continuità delle funzioni connesse alle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale. E' stata prevista la creazione in Telecom Italia di una cosiddetta "organizzazione di sicurezza", ovvero una funzione aziendale autonoma e indipendente dal vertice societario, volta a garantire l'attuazione delle prescrizioni governative.

Tra le prescrizioni di carattere generale contenute nel d.P.C.M. del 16 ottobre 2017, alcune hanno riguardato il mantenimento stabile sul territorio nazionale delle funzioni di gestione e sicurezza delle reti e dei servizi e delle forniture che supportano attività "strategiche", altre sono volte a garantire la continuità delle funzioni connesse alle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale. Sono state, inoltre, previste condizioni volte ad assicurare assetti organizzativi dedicati alle attività aziendali rilevanti per la sicurezza nazionale, prevedendone la piena autonomia sia sotto il profilo economico-finanziario che di gestione del personale, attraverso l'assegnazione di una dotazione di risorse umane, finanziarie e strumentali idonee a garantirne l'indipendenza (è stata prevista in concreto la creazione di una "organizzazione di sicurezza", ovvero

[176] Decreto-legge 31 marzo 2011, n. 34, Disposizioni urgenti in favore della cultura, in materia di incroci tra settori della stampa e della televisione, di razionalizzazione dello spettro radioelettrico, di moratoria nucleare, di partecipazioni della Cassa depositi e prestiti, nonché per gli enti del Servizio sanitario nazionale della regione Abruzzo, convertito con modificazioni dalla L. 26 maggio 2011, n. 75, in GU 27 maggio 2011, n. 122.

una funzione aziendale autonoma e indipendente dal vertice societario, volta a garantire l'attuazione delle prescrizioni governative).

3.8.9. Il 5G e la nozione di "soggetto esterno" all'Unione europea

Come rilevato, con il decreto legge n. 22/2019 del 25 marzo 2019 l'ombrello protettivo del *Golden Power* è stato esteso al 5G.

Le sue previsioni risultano particolarmente innovative in quanto ora il *Golden Power* non si applica soltanto ai mutamenti proprietari bensì anche a questioni eminentemente operative, come per esempio l'acquisto di determinati apparati per accendere la rete 5G. Sono infatti ricompresi nell'ambito oggettivo di applicazione diverse fattispecie legate alla nuova tecnologia, come gli appalti e le forniture commerciali di beni o servizi relativi alla progettazione, realizzazione, manutenzione e gestione delle reti.

Esse da una lato confermano l'applicabilità dei veti normativi ai soggetti extra-UE, dall'altro forniscono una definizione ampia di "*soggetto esterno all'Unione europea*" in chiave anti elusiva. La definizione di soggetto esterno all'Unione europea è fornita dal comma 3 dell'articolo 1-bis e comprende, oltre alle persone fisiche e giuridiche stabilite fuori dello spazio economico europeo (soggetti esterni in senso stretto), quelle in esso stabilite ma controllate direttamente o indirettamente da soggetti esterni, nonché quelle che siano stabilite in Europa al fine di eludere l'applicazione della disciplina in argomento.

E' prevista la valutazione del Comitato interministeriale incardinato presso la Presidenza del Consiglio, analogamente a quanto già accade (previo obbligo di notifica), di tutte le acquisizioni di componenti ad alta intensità tecnologica funzionali alla realizzazione o alla gestione del 5G. Sono oggetto di valutazione anche gli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano.

L'estensione del *Golden power* al 5G appare senza dubbio condivisibile nell'ottica di proteggere una tecnologia che, come rilevato, è destinata a rivestire un ruolo fondamentale per l'economia e la società del prossimo futuro. Tuttavia nella previsione normativa non sono indicati i criteri sui quali dovrà fondarsi l'eventuale decisione di esercitare il potere di veto o di imporre specifiche prescrizioni o condizioni. Il che induce a ritenere che si tratti di uno strumento giuridico dall'indubbio carattere dissuasivo ma che potrà essere utilizzato con cautela, nel rispetto dei principi di proporzionalità e non discriminazione. D'altronde – come rilevato - si tratta di esercitare prerogative di esclusiva competenza nazionale, ancorate a parametri che non sono suscettibili di definizione *ex ante* e si traducono nell'individuare di volta in volta le attività che rivestono rilevanza strategica valutando in modo adeguato i rischi per la difesa e la sicurezza nazionale.

3.8.10. La possibilità di intervenire sui contratti 5G già conclusi

Il decreto-legge 21 settembre 2019, n. 105[177], convertito in legge n. 133 del 2019 sul perimetro di sicurezza nazionale cibernetica ha esteso l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori strategici, coordinandolo con l'attuazione del regolamento 2019/452 in materia di controllo degli investimenti esteri diretti.

In particolare l'art. 3 detta disposizioni di raccordo tra le previsioni della legge sul perimetro di sicurezza nazionale cibernetica e la disciplina dei poteri speciali in tema di 5G. Si prevede che le norme della legge citata si applichino ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, anche per i contratti o gli accordi, ove conclusi con soggetti esterni all'Unione europea, relativi ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

Dalla data di entrata in vigore del regolamento previsto dalla stessa legge n. 133/2019 (da adottarsi ai sensi dall'art. 1, comma 6) relativo a procedure, modalità e termini per l'affidamento di forniture di beni e servizi ICT, i poteri speciali inerenti le reti sono esercitati previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità, che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, da parte dei centri di valutazione (quello nazionale istituito presso il Ministero dello sviluppo economico e quello del Ministero della difesa).

Viene poi prevista una disciplina transitoria, con la possibilità di ridefinire, nel termine di sessanta giorni dalla data di entrata in vigore del regolamento citato, le condizioni o le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati.

In particolare, possono essere modificate o integrate con misure aggiuntive necessarie ad assicurare livelli di sicurezza equivalenti a quelli previsti dal decreto-legge in esame le condizioni e le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati con decreti del Presidente del Consiglio dei ministri - e adottati sulla base della normativa sui poteri speciali in data anteriore alla data di entrata in vigore del medesimo regolamento -, qualora attinenti alle reti, ai sistemi informativi e ai servizi informatici inseriti negli elenchi dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica.

Si dispone infatti che qualora, a seguito delle valutazioni svolte dai centri di valutazione, emergano elementi indicanti fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, possono essere disposte misure aggiuntive anche prescrivendo, qualora indispensabile al fine di risolvere le vulnerabilità accertate, la sostituzione di apparati e di prodotti.

[177] Decreto-legge 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, convertito con modificazioni dalla L. 18 novembre 2019, n. 133, in G.U. 20 novembre 2019, n. 272.

Si tratta di una previsione importante, che consente al governo di intervenire con riferimento ai contratti già conclusi, addirittura ordinando alle imprese la sostituzione degli apparati e prodotti non sicuri. La possibilità di fare uso di tale strumento è tuttavia consentita solo qualora si tratti di misura indispensabile.

L'art. 4-bis estende il termine per l'esercizio dei poteri speciali da parte del Governo, con l'indicazione di ulteriori elementi informativi che devono essere resi dalle imprese detentrici degli *asset* strategici; viene ampliato l'oggetto di alcuni poteri speciali e sono modificati e integrati gli obblighi di notifica finalizzati all'esercizio dei poteri speciali.

La disciplina dei poteri speciali relativa al 5G viene leggermente rivista così da rendere il procedimento sostanzialmente simmetrico a quello previsto per i settori della difesa e della sicurezza nazionale. E' ridefinito il concetto di "soggetto esterno all'Unione europea" e sono precisati i criteri per determinare se un investimento estero sia suscettibile di incidere sulla sicurezza o sull'ordine pubblico. Viene inoltre sottoposta all'obbligo di notifica l'acquisizione a qualsiasi titolo (in luogo del solo acquisto) di beni o servizi relativi alle reti 5G, qualora posti in essere con soggetti esterni all'Unione europea.

Sono quindi introdotte ulteriori circostanze che il Governo può tenere in considerazione per l'esercizio dei poteri speciali, nel caso in cui l'acquirente di partecipazioni rilevanti sia un soggetto esterno all'Unione europea.

3.8.11. L'estensione del *Golden Power*

L'obiettivo di proteggere il sistema economico nazionale indebolito dall'emergenza Covid-19 e tutelare i suoi *asset* pregiati ha indotto il governo a integrare, con l'art. 15 del decreto legge "Liquidità" n. 23 dell'8 aprile 2020[178], le norme vigenti in tema di *Golden Power*.

La previsione normativa, simile a quella adottata da Germania e Spagna, benché contenuta in un solo articolo, risulta tecnicamente complessa e articolata.

Raccogliendo le indicazioni del Copasir (Comitato parlamentare per la sicurezza della Repubblica) in data 25 marzo 2020 e sulla scia delle linee guida di cui alla raccomandazione della Commissione europea del 25 marzo 2019, il governo con tale intervento in sostanza ha anticipato la valutazione prevista dal regolamento europeo 2019/452 sul controllo degli investimenti esteri (applicabile dall'11 ottobre 2020), con la possibilità di adottare misure restrittive a protezione di sicurezza e ordine pubblico.

Allarga infatti l'ombrello protettivo del *Golden Power*, finora limitato a difesa e sicurezza nazionale, energia, trasporti e comunicazioni, ai settori riguardati dal

178 Decreto-legge 8 aprile 2020, n. 23, Misure urgenti in materia di accesso al credito e di adempimenti fiscali per le imprese, di poteri speciali nei settori strategici, nonché interventi in materia di salute e lavoro, di proroga di termini amministrativi e processuali, in GU n. 94 dell'8 aprile 2020.

citato regolamento europeo, attribuendo al governo un potere rilevante e dalle delicate implicazioni, ancorché per un periodo limitato (fino al 31 dicembre 2020).

Le disposizioni contenute nel decreto legge non incidono tuttavia sulla supervisione già assicurata al governo sul 5G in virtù della legge n. 41/2019 e della legge sul perimetro di sicurezza n. 133/2019. In tal senso i contratti e gli accordi relativi all'acquisizione di beni e servizi relativi alla progettazione, realizzazione, manutenzione e gestione della rete 5G continuano pertanto riguardati dalle citate previsioni normative; tuttavia le operazioni societarie relative al 5G possono rientrare nel raggio d'azione della nuova previsione.

Il tempo di risposta del comitato *Golden Power* è di 45 giorni, salvo le proroghe previste; per le operazioni relative alla rete 5G (i contratti e gli accordi citati) si applica invece il termine di 30 giorni.

Come rilevato, il decreto legge estende gli obblighi relativi al *Golden Power* a beni e rapporti nei settori riguardati dal regolamento europeo. Si applica pertanto alle infrastrutture critiche, siano esse fisiche o virtuali, tra cui l'energia, i trasporti, l'acqua, la salute, le comunicazioni, i media, il trattamento o l'archiviazione di dati, le infrastrutture aerospaziali, di difesa, elettorali o finanziarie, e le strutture sensibili, nonché gli investimenti in terreni e immobili fondamentali per l'utilizzo di tali infrastrutture, tecnologie critiche e prodotti a duplice uso, tra cui l'intelligenza artificiale, la robotica, i semiconduttori, la cybersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie. Sono riguardati anche la sicurezza dell'approvvigionamento di fattori produttivi critici, tra cui l'energia e le materie prime, nonché la sicurezza alimentare, l'accesso a informazioni sensibili, compresi i dati personali, o la capacità di controllare tali informazioni, la libertà e pluralismo dei media. Tutti i settori citati assumono pertanto rilevanza strategica e in essi operano un vasto numero di società, ivi comprese molte PMI.

Le nuove norme sul *Golden Power* previste dal decreto legge si applicano ai soggetti UE solo nel caso in cui l'acquisto di partecipazione sia rilevante e determini l'insediamento stabile dell'acquirente in ragione dell'assunzione di controllo della società.

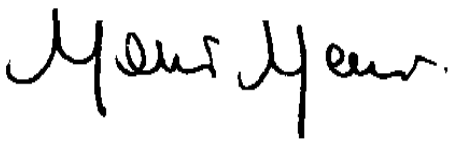
È previsto invece l'obbligo di notifica, da parte di un soggetto esterno all'UE, di un acquisto di partecipazioni che attribuiscono una quota dei diritti di voto o di capitale superiore al 10% e il valore complessivo dell'investimento è pari o superiore a 1 milione di euro.

In base alle nuove disposizioni il governo ha la possibilità di intervenire d'ufficio anche senza notifica. Lo Stato si riserva infatti di intervenire d'ufficio qualora venga a conoscenza di operazioni poste in essere fino al 31 dicembre 2020, a prescindere dal fatto che la notifica sia avvenuta o meno. In tal caso si applica il termine di 45 giorni e l'eventuale decisione di divieto sarà adottata con decreto del Presidente del Consiglio dei Ministri. La Presidenza del Consiglio dei Ministri e la società non hanno l'obbligo di dare comunicazione al pubblico dell'operazione ai sensi del testo unico

della finanza. E' peraltro previsto che in presenza di disposizioni specifiche inerenti ad altri settori, volte a garantire la tutela degli stessi interessi essenziali dello Stato perseguiti dalle norme sul *Golden Power*, si applichino le prime in quanto "*lex specialis*".

L'obbligo di notifica dell'acquisto di partecipazioni finanziarie in tutti i settori ivi riguardati si applica sino al momento in cui, con decreto, il Presidente del Consiglio dei Ministri indicherà i beni e i rapporti di rilevanza strategica per l'interesse nazionale ulteriori rispetto a quelli già individuati nei settori di difesa e sicurezza nazionale, energia, trasporti e comunicazioni. Tutte le altre misure previste, relative per esempio a delibere, atti o operazioni che modificano la titolarità, il controllo o la disponibilità degli attivi delle società, hanno invece come scadenza il 31 dicembre 2020, compreso il potere di intervento d'ufficio del governo.

Roma, 15 maggio 2020



Riferimenti bibliografici

BALDONI R. – MONTANARI L. – QUERZONI L. (a cura di), *2016 Italian Cybersecurity Report. Controlli Essenziali di Cybersecurity,* (a cura di) *Cis Sapienza*. Laboratorio Nazionale CINI di Cybersecurity - Consorzio Interuniversitario Nazionale per l'Informatica, Versione 1.0, marzo 2017.

BARNARD-WILLS D., *This is not a Cyber war, its a...? Wikileaks, Anonymous and the Politics of Hegemony*, in *Proceedings of the 10th European Conference on Information Warfare and Security: The Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia 7-8 July 2011*. Academic Conferences Limited, 2011.

BAUMANN M.O. - SCHÜNEMANN W.J., *Introduction: Privacy, Data Protection and Cybersecurity in Europe*, in *Privacy, Data Protection and Cybersecurity in Europe*. Springer International Publishing, 2017.

CARRAPICO H. –BARRINHA A., *The EU as a coherent (cyber) security actor?*, in *JCMS: Journal of Common Market Studies*, 2017.

CHRISTOU G., *Network and Information Security and Cyber Defence in the European Union, Cybersecurity in the European Union*. Palgrave Macmillan UK, 2016.

CHRISTOU G., *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Palgrave Macmillan, 2016.

DE FALCO M., *Stuxnet Facts Report - A Technical and Strategic Analysis*, NATO CCD COE Publications, 2012.

EDGETT S. J., *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy,* in *Pepp. L. Rev.* 30, 2002.

HARTMANN U., *The Evolution of the Hybrid Threat, and Resilience as a Countermeasure*, NATO Research Paper, 2017.

HATHAWAY O. A. (et al.), *The Law of Cyber-Attack*, *Yale Law School*, novembre 2011.

KREPS S. –DAS D., *Warring from the virtual to the real: Assessing the public's threshold for war over cyber security*, in *Research & Politics* 4.2, 2017

LAWRENCE SLOAN D., *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation,* in *Duke Law Journal,* 2001.

LEE S., "*The Cybersecurity Implications of Chinese Undersea Cable Investment*" *East Asia Center, University of Washington,* febbraio 2017.

MENSI M., *Il caso "Datagate". Alcune riflessioni*, in *Diritto, economia e tecnologia della privacy*, 1, 2013.

MENSI M., *Minaccia cyber, sicurezza nazionale e profili giuridici*, in *Lo spazio cyber e cosmico - Risorse dual use per il sistema Italia in Europa*, Roma 2019

MENSI M., *5G e la Cina. Quali regole per proteggere le nostre infrastrutture critiche,* in *Agenda digitale,* 10 aprile 2019

MENSI M. – FALLETTA P., *Il diritto del Web*, Padova, 2018.

MOROZOV E., *To save everything, click here. Technology, solutionism, and the urge to fix problems that don't exist*, UK, 2013.

NAPOLITANO G., *Il Regolamento sul controllo degli investimenti esteri diretti: alla ricerca di una sovranità europea nell'arena economica globale*, in *Rivista della regolazione dei mercati*, n. 1, 2019.
PERKOVICH G. – LEVITE A. E., *Understanding Cyber Conflict, 14 Analogies*. Georgetown University Press, 2017.
PORCHE I. R. - SOLLINGER J. M. - MCKAY S., *A Cyberworm that Knows no Boundaries*, Rand Occasional Paper, Santa Monica (Ca), 2011.
RAPETTO U., *Le sfide alla sicurezza nell'era digitale*, Nomos & Khaos, Roma, 2013.
REIDELBERG J. R., *The data surveillance state in the United States and Europe, Wake Forest Law Review*, Vol. 49, No. 2, Summer 2014.
ROUSSI A., *China charts a path to Europe, Nature* Vol. 569, May 2019.
RUOHONEN J. – HYRYNSALMI S. – LEPPÄNEN V., *An outlook on the institutional evolution of the European Union cyber security apparatus*, in *Government Information Quarterly* 33.4, 2016.
SMYTH J., "*Huawei's undersea cable project raises red flag in Australia*," *Financial Times,* dicembre 2017.
SWP, Stiftung Wissenschaft und Politik , German Institute for International and Security Affairs , China guided memory, No. 4, February 2020.
TAPPERO MERLO G., *Soggetti e ambiti della minaccia cibernetica: dal sistema paese alle proposte di cyber governance*? in *La Comunità Internazionale*, Fasc. 1/2012.
VAN DER MEULEN N. - A JO E. –SOESANTO S., *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses,* Studio commissionato dal Parlamento europeo, 18 novembre 2015.
VAN HOBOKEN J.V. - J., RUBINSTEIN I. S., *Privacy and Security in the Cloud: some realism about technical solutions to transnational surveillance in the post-Snowden era*, *Maine Law Review*, Vol. 66, n.2, 2014.
WEBER R. H. –STUDER E., *Cybersecurity in the Internet of Things: Legal aspects*, in *Computer Law & Security Review* 32.5, 2016.
5G AMERICAS WHITE PAPER, *The Evolution of Security in 5G,* July 2019.