LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Scienze politiche
Corso di Relazioni internazionali
Cattedra di Organizzazione internazionale e diritti umani

Il *cyber space*: una nuova dimensione per la conflittualità e la tutela dei diritti umani

Relatore:

Francesco Cherubini

Candidato: Giada Farina

Matricola: 626762

Correlatrice:

Maria Beatrice Deli

Anno Accademico: 2016-2017

Ai miei genitori,

che con la loro dolcezza e pazienza mi hanno incoraggiato a non mollare mai e a dare sempre il massimo.

Ai miei amici di sempre e a quelli che ho incontrato in questi cinque anni,

che hanno creduto in me e che mi hanno sostenuto fino al raggiungimento di questo traguardo.

A questa splendida Università, a tutto il personale che ne fa parte e, in particolar modo, al mio relatore,

rivolgo un pensiero ed un ringraziamento per aver contribuito in maniera determinante alla mia crescita personale e professionale, consentendomi di fare esperienze straordinarie e nuovi incontri indimenticabili.

Indice

Introduzione……..5

CAPITOLO I

IL *CYBER* SPAZIO: LE NUOVE FRONTIERE DELLA SICUREZZA

1.1 I concetti di *cyber* spazio, *cyber security*, *cyber crime* e *cyber attack*…….8

1.2 Le infrastrutture critiche come bersaglio…….17

1.3 La strategia dell'Unione europea in materia di *cyber defence*…….23

1.4 La normativa vigente in ambito cyber in Italia……...33

CAPITOLO II

IL NUOVO FENOMENO DELLA *CYBER WAR* E LE IMPLICAZIONI DAL PUNTO DI VISTA DEL DIRITTO INTERNAZIONALE

2.1 Applicazione dello *jus ad bellum* e dello *jus in bello* alla luce del concetto di *cyber war*……44

2.2 Le Nazioni Unite e il mantenimento della pace e della sicurezza internazionali…….48

2.3 *Cyber attacks*: cosa dice la Carta delle Nazioni Unite……...55

2.4 Il regime di responsabilità internazionale……...65

2.5 Principio di sovranità territoriale, responsabilità internazionale e *cyber attacks*……73

CAPITOLO III

TUTELA DEI DIRITTI UMANI NELL'AMBITO DELLA *CYBER SECURITY*

3.1 Il regime giuridico internazionale a tutela dei diritti umani……...81

3.2 La tutela dei diritti umani a livello regionale: il sistema europeo……93

3.3 *Cyber security* e tutela dei diritti umani……..98

3.4 *Privacy* vs Sicurezza……...…..116

3.5 Dalla Carta di Nizza al General Data Protection Regulation ……..…….122

Conclusione……...131

Bibliografia……134

Introduzione

Il XXI secolo è anche noto come l'era dell'*information society* [1](società dell'informazione), espressione impiegata da alcuni sociologi per indicare la moderna società post-industriale nella quale l'informatica e le telecomunicazioni hanno assunto il ruolo di protagoniste.
La moderna 'società dell'informazione' è, perciò, una società in cui l'economia si basa prevalentemente sulla produzione di beni o servizi che hanno a che fare con la tecnologia delle informazioni e rilevante è il valore economico della conoscenza come risorsa strategica.
Con l'avvento di Internet hanno avuto, poi, origine cambiamenti epocali nella sfera delle interazioni sociali, in quella delle strategie militari e, infine, nell'ambito della tutela dei diritti umani.
Convenzionalmente, per indicare l'ambiente nel quale avvengono le operazioni che fanno uso di Internet si utilizza il termine *cyber space*, che sarà analizzato più nel dettaglio nel primo capitolo di questa tesi.
Brevemente, possiamo dire che esso consiste in uno spazio virtuale privo di confini fisici, di limiti geografici e di un'autorità centrale di governo, al quale si può accedere mediante dispositivi in grado di collegarsi ad una rete informatica, in qualsiasi parte del mondo ci troviamo.
Esso è, dunque, in grado di interconnettere a livello planetario gli utenti che vi operano e di trasportare un enorme 'bagaglio' di dati e di informazioni in un arco temporale brevissimo.
È importante porre l'accento, tuttavia, anche sugli aspetti negativi che lo caratterizzano: infatti, i sistemi al suo interno sono stati inizialmente sviluppati pensando a come facilitare l'uomo nelle sue attività quotidiane, senza tener conto delle criticità e degli aspetti legati alla sicurezza che sono sempre più oggetto di discussione tra gli esperti, data l'alta vulnerabilità delle reti informatiche spesso sfruttate in modo criminoso.
In un sistema economico globale nel quale le informazioni hanno un valore essenziale, la sicurezza delle reti è diventata, pertanto, una delle sfide più serie per il settore economico e, in generale, per gli Stati.
I crimini informatici sono oltremodo ardui da prevedere così come è impossibile conoscere i loro effetti nel medio/lungo termine, il che rende il *cyber crime* più conveniente da vari punti di vista.

> Non può quindi stupire il progressivo incremento, quantitativo e qualitativo, di attacchi e minacce criminali con le finalità più disparate, in quella 'terra di mezzo' che è oramai diventato il *cyber space*: dalle frodi e dalle estorsioni informatiche ai furti di identità e di dati sensibili, fino ad arrivare allo spionaggio e al sabotaggio, compresi gli atti vandalici meramente emulativi. Attacchi che possono anche non essere mirati a colpire un soggetto preciso, selezionato in base a determinate caratteristiche, ma a danneggiare in modo

[1] KULESZA, BALLESTE (2015: xiii).

casuale un numero indefinito di soggetti sensibili alla minaccia predisposta dal criminale[2].

A fronte di ciò, gli Stati si sono via via impegnati nell'elaborazione di nuove politiche nazionali nel campo della *cyber security*, al fine di proteggere se stessi e i propri cittadini da attacchi informatici quali furto e manipolazione di dati sensibili, contraffazione, frodi, manomissione dei sistemi comunicativi, attacchi a infrastrutture critiche nazionali, estorsione, *cyber* spionaggio e *cyber intelligence*.
Per contrastare tali atti è necessario, comunque, anche un intervento a livello internazionale. Questo perché le sole politiche nazionali non sono in grado di avere effetti al di fuori dei confini territoriali di uno Stato, diversamente da ciò che attori statali e non statali riescono a fare nel *cyber space*: le peculiarità che lo caratterizzano, di fatto, consentono di agire in ogni luogo del mondo e di attaccare anche a miglia di distanza aggirando, senza alcun problema, il principio di sovranità territoriale.
Nella lotta contro i *cyber crimes* e i *cyber attacks*, altrettanto rilevante è la questione relativa alla tutela dei diritti umani e, in particolare, del diritto alla libertà di espressione e del diritto alla riservatezza.
Appare necessario, quindi, attuare misure di sicurezza tali da assicurare al contempo la protezione dei diritti dell'uomo, oltre che la protezione dei sistemi informativi o degli Stati stessi.
Anche in questo settore una collaborazione tra i membri della Comunità internazionale potrebbe garantire ulteriormente:

a) l'accesso universale a Internet, che dovrebbe, di fatti, essere assicurato da tutti gli Stati in considerazione dell'idea del *cyber* spazio come bene comune*;*
b) un'efficace *data information sharing*, al fine di consentire lo scambio di informazioni e dati intra e inter Stati nel rispetto del diritto alla riservatezza di cui godono i singoli individui.

Il presente elaborato si propone di trattare tali argomenti e di offrire una panoramica dei fenomeni attinenti il *cyber* spazio e delle problematiche ad essi connesse.
Il primo capitolo sarà dedicato all'illustrazione dei concetti di *cyber* spazio, *cyber security*, *cyber crime* e *cyber attack*. Inoltre, si analizzeranno le strategie in ambito *cyber* dell'Unione europea e dell'Italia.
Il secondo capitolo si concentrerà sul concetto di *cyber war* con lo scopo di illustrare questo nuovo fenomeno, comprendere quali sono gli attori che entrano in gioco e quali le sue conseguenze e peculiarità.
In questa prospettiva, saranno esaminate, inoltre, le norme di diritto internazionale che disciplinano l'uso della forza nella Comunità

[2] BALDONI, DE NICOLA (2015: 1 ss.).

internazionale al fine di stabilire se esse trovino applicazione anche nell'ambito di questa nuova sfera di conflittualità.
Infine, nel terzo capitolo analizzeremo i vigenti sistemi di protezione dei diritti umani e, nello specifico, del diritto alla libertà di espressione e del diritto alla *privacy*. In tale contesto, saranno analizzate le posizioni di coloro che sostengono la tesi secondo cui una maggiore tutela dei diritti umani comporterebbe una minore capacità degli Stati di garantire sicurezza e di coloro che ritengono possibile, al contrario, pervenire ad un bilanciamento tra la necessità di tutelare i diritti umani e il bisogno di assicurare il perseguimento di efficaci politiche di sicurezza nazionale ed informatica, dove un'esigenza è complementare per il raggiungimento dell'altra.

CAPITOLO I

IL *CYBER* SPAZIO: LE NUOVE FRONTIERE DELLA SICUREZZA

1.1 I concetti di *cyber* spazio, *cyber security*, *cyber crime* e *cyber attack*

Il termine *cyber* spazio fu coniato per la prima volta dallo scrittore canadese William Gibson e utilizzato all'interno del suo racconto 'La notte che bruciammo Chrome' (*Burning Chrome*), pubblicato nel 1982 sulla rivista Omni; fu, in seguito, inserito nel suo romanzo 'Neuromante' e, così, reso noto al pubblico. Egli descrisse il *cyber* spazio come:

> un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici [...] Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano [...].

Successivamente, Gibson dichiarerà che la fusione dei due termini '*cyber information'* e '*space'* rappresentò per lui la creazione di un nuovo termine indicativo di un qualcosa di unico, privo di qualsiasi significato semantico vero e proprio eppure adatto a descrivere quella realtà virtuale che egli si prefigurava nella mente.
Tale termine assunse un significato più vicino a quello che oggi gli attribuiamo soltanto negli anni Novanta, con la nascita di Internet. Esso fu, infatti, impiegato per indicare quel luogo virtuale in cui la comunicazione attraverso le reti informatiche avveniva.
Una più recente definizione di *cyber space* è stata, invece, fornita dal Pentagono, che nel 2008 ha voluto riunire una commissione di esperti del settore affinché elaborasse una definizione univoca e condivisa di tale termine. Questa è arrivata soltanto un anno più tardi e provvede a definire il *cyber* spazio come:

> the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers[3].

In altre parole, il *cyber* spazio non è altro che il regno delle reti informatiche (e degli utenti dietro queste) nel quale le informazioni vengono immagazzinate, memorizzate, condivise e diffuse.

[3] SINGER, FRIEDMAN (2014: 12).

Ad ogni modo, ciò che più a noi interessa è capire quali siano le caratteristiche essenziali del *cyber* spazio e perché esso sia unico nel suo genere.
Iniziamo con l'osservare la sua prima tipicità: l'uso dell'elettronica e dello spettro elettromagnetico. Ne deriva che la sua caratteristica principale è l'essere una realtà astratta che connette ad un'unica rete i computer di tutto il mondo consentendo agli utenti che ne fanno uso di interagire tra loro.
Tuttavia, pur mantenendo questa sua essenzialità, il *cyber* spazio non è da considerarsi un mondo puramente virtuale poiché accedere ad una connessione richiede, comunque, la presenza di oggetti fisici (dispositivi come computer, telefoni cellulari o *tablet*). Inoltre, dietro a tali dispositivi vi sono degli individui che influenzano e plasmano questo mondo, che condividono informazioni e che, a loro volta, vengono 'formati' da esso e stimolati al progresso tecnologico.
Il *cyber space* è da ritenersi, perciò, un mondo caratterizzato dal dinamismo e in continua trasformazione. Il *know-how* dell'uomo consente, infatti, la produzione di tecnologie sempre più avanzate, nuovi dispositivi connessi alla rete e, nel complesso, la creazione di un mondo interconnesso e interdipendente.
Secondo Even Shmuel, pertanto, nel *cyber space* coesistono tre diversi elementi:

- *the human layer*, vale a dire le risorse umane dedite all'utilizzo dei sistemi di informatizzazione e comunicazione;
- *the logical layer*, ossia i programmi/*software*, i sistemi operativi e le varie applicazioni e, infine, i bit che viaggiano nell'etere;
- *the physical layer*, ovvero le infrastrutture e le apparecchiature fisiche mobili o fisse, che rendono possibile la trasmissione di dati[4].

Si aggiunga un'ulteriore considerazione: l'evoluzione di Internet ha esteso Internet stesso ad oggetti e luoghi reali che ora possono connettersi alla rete e trasferire dati e informazioni. Tale fenomeno è indicato con l'espressione *Internet of Things* (IoT), che sta a designare proprio la diffusione di oggetti di uso comune collegati alle reti informatiche, il cui ambito di applicazione risulta ad oggi essere molto vasto.
Attualmente, i settori di più interesse sono la domotica (scienza interdisciplinare che si occupa dello studio delle tecnologie atte a migliorare la qualità della vita nella casa e più in generale negli ambienti antropizzati), la sorveglianza o il settore dei trasporti. In riferimento a quest'ultimo pensiamo alle auto moderne: esse non sono più dei dispositivi meramente meccanici; al contrario, sono sempre più frequentemente dotate di sistemi computerizzati altamente tecnologici che, non soltanto migliorano la qualità di guida e di assistenza al guidatore, ma permettono all'automobile stessa di connettersi con il mondo esterno. Se da un lato ciò ha consentito un

[4] EVEN, SIMAN-TOV (2012: 10).

miglioramento del livello di sicurezza al volante (pensiamo ai sistemi di frenata automatici di emergenza, cosiddetti *Autonomous Emergency Braking*, che contribuiscono alla riduzione di incidenti essendo in grado di frenare automaticamente la vettura), dall'altro è più alta la probabilità che si verifichi un'intrusione nei e un'alterazione dei sistemi di bordo con lo scopo di prendere il controllo del veicolo. Questa minaccia è ancor più seria se consideriamo l'ipotesi in cui un attacco di questo tipo possa essere eseguito remotamente attraverso le varie interfacce di comunicazione del veicolo con il mondo esterno, quali dispositivi mobili (lettori MP3, palmari o *tablet*) e *smartphones*.

Allo stesso modo, nel settore dell'aviazione civile e commerciale si sta diffondendo l'idea di produrre nel futuro un maggior numero di *e-enabled aircrafts*, aeromobili in grado di operare in maniera autonoma e intelligente attraverso la connessione e interconnessione tra i sistemi posizionati in aria, a terra e nello spazio. Nuovamente, nonostante i vantaggi di tanta tecnologia, si palesa il timore di attacchi cibernetici (sia contro gli aeromobili sia contro le infrastrutture di controllo del traffico aereo) potenzialmente lesivi per la sicurezza di un Paese e dei suoi cittadini.

Occorre tener conto, infine, anche di fenomeni quali l'*e-commerce* (vale a dire la possibilità di effettuare acquisti direttamente *on-line* in qualsiasi posto noi ci troviamo) o l'*e-banking* (l'insieme di transazioni bancarie condotte attraverso terminali connessi a internet), che permettono una gestione dei propri interessi attraverso le reti informatiche e che mostrano come ormai viviamo in un mondo sempre più tecnologico e interconnesso. Anche in questo settore gli utenti possono essere vittime di attacchi informatici, per lo più finalizzati al furto di dati o di denaro, ed è richiesta dunque l'attuazione di misure di sicurezza adeguate a far fronte a tale minaccia.

Ciò detto perciò, sebbene la produzione di dispositivi IoT possa facilitare la gestione di attività quotidiane, innumerevoli sono i rischi legati al loro impiego. Da tale considerazione emerge, allora, la necessità di proteggersi.

Il termine *cyber security* è, nell'era contemporanea, frequentemente utilizzato dagli ambienti militari, dai media, dalle imprese private per indicare proprio il bisogno di difendersi all'interno dell'immenso spazio cibernetico. Non esiste al momento una definizione universalmente riconosciuta di tale termine; procediamo, allora, individuando quelle più note e maggiormente condivise dagli esperti.

Secondo Joanna Kulesza, il concetto di *cyber security* indica allo stesso tempo la necessità di introdurre determinate misure di sicurezza per contrastare i cosiddetti reati informatici e la garanzia di tutela di determinati diritti e libertà individuali[5]. Dunque, quando si parla di *cyber security* si vuol far riferimento tanto alle misure di protezione contro attacchi informatici quanto alla necessità di assicurare la protezione dei diritti degli individui (pensiamo al diritto alla *privacy*).

[5] KULESZA, BALLESTE (2015: 1).

Una definizione più precisa è stata fornita dall'ITU (l'International Telecommunication Union[6]) che ha presentato la *cyber security* come:

> the collection of tools, policies, security concepts […] approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets[7].

L'Unione europea ha, invece, offerto una definizione più generale affermando che essa è l'insieme di

> safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure[8].

L'Internet Society (ISOC) ha sottolineato che la *cyber security* è

> a catchword [che è] frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and solutions ranging from the technical to the legislative[9].

Sebbene queste definizioni siano diverse tra loro, tutte condividono una premessa: non vi è soltanto il bisogno di proteggersi da un generale pericolo ma anche la presenza di un avversario dal quale difendersi, seppur spesso non ben identificato. Tale premessa costituisce la ragione per cui possiamo parlare di questioni di *cyber security* solo e soltanto quando un'attività perpetrata da uno o più individui avviene mediante l'utilizzo di reti informatiche e minaccia la sicurezza di un Paese.
Per questa ragione, non è sufficiente un semplice mal funzionamento dei sistemi informativi di un Paese, delle sue infrastrutture, delle reti di calcolatori e/o dispositivi elettronici personali ma è, altresì, necessaria la presenza di una o più persone che volontariamente alterino la sicurezza di tali sistemi. Un'efficace strategia di *cyber security* richiede, allora, un'analisi delle minacce, delle vulnerabilità e dei rischi associati all'impiego di sistemi informatici nonché l'attuazione di adeguate e specifiche misure difensive.
Quando parliamo di misure di *cyber security* è bene ricordare che queste possono consistere tanto in misure di prevenzione, le quali agiscono riducendo la probabilità di realizzazione di una minaccia, quanto in misure di protezione, le quali agiscono riducendo la gravità del danno prodotto da un attacco o da un crimine informatico.

---

[6] Organizzazione internazionale, fondata a Parigi nel 1865, che si occupa di definire gli standard nelle telecomunicazioni e nell'uso delle onde radio. Dal 1947 è una delle agenzie specializzate delle Nazioni Unite.
[7] Raccomandazione dell'International Telecommunication Union, del 18 aprile 2008, X.1205 su *data networks, open system, communications and security*.
[8] Comunicazione congiunta della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 7 febbraio 2013, n. 6225.
[9] GREEN, ROSSINI (2015: 2).

Strettamente legato al concetto di *cyber security* è quello di *cyber crime*, vale a dire l'insieme delle azioni commesse in violazione della legislazione internazionale e nazionale (laddove presente) che implicano l'utilizzo di computer o reti informatiche[10]. Anche in questo caso non abbiamo una definizione univoca di tale termine. Soffermiamoci su quelle più note.
A livello internazionale, la Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001 fa riferimento ad un elenco non tassativo di attività considerate come crimini informatici[11]; rientrano tra questi reati la violazione di contenuti e del diritto d'autore, l'acquisizione di dati riservati, la frode e la pedopornografia.
Nello stesso modo procede il Manuale delle Nazioni Unite sulla prevenzione e il controllo del crimine informatico (*The United Nations Manual on the Prevention and Control of Computer Related Crime*), il quale elenca una serie di reati classificati come *cyber crimes*[12].
Solitamente i *cyber crimes* perseguono interessi privati, quali soprattutto il guadagno economico per i loro responsabili, diversamente da quel che accade nel caso di un *cyber attack*. Infatti, sebbene questo termine venga spesso equiparato a quello di *cyber crime*, in realtà esso indica un fenomeno ben diverso.
L'attacco informatico rappresenta sempre un'azione, come si può facilmente intuire, perpetrata mediante l'utilizzo di computer e *networks*; tuttavia a cambiare è l'obiettivo, che consiste nell'indebolire o neutralizzare i sistemi computerizzati oggetto di attacco. Dietro di esso, inoltre, si cela la volontà di compromettere seriamente la sicurezza nazionale di un Paese . Il fine ultimo è quello di causare una paralisi della vittima, dimostrarne pubblicamente la fragilità, disseminare terrore negli individui[13].
La caratteristica principale di un *cyber attack* è quella di essere per l'appunto un attacco, ossia il prodotto di una condotta attiva, sia che si parli di offesa attiva sia che si parli di difesa. In quest'ultimo caso, gli Stati, per lo più, adottano una serie di contromisure elettroniche finalizzate a colpire quei sistemi che stanno compiendo un attacco informatico in modo da arrestarne la realizzazione. Sono da escludere, invece, da tale categoria tutti quei sistemi di difesa passiva, spesso impiegati dagli Stati, quali ad esempio i *software* antivirus o i *firewalls* (componente di difesa perimetrale di una rete informatica volto a controllare gli accessi alle risorse di un sistema e a gestire il flusso di informazione che tale sistema scambia con l'esterno).
La seconda caratteristica da tenere bene a mente riguarda il fine ultimo dell'attacco informatico, che permette di distinguerlo da un semplice crimine informatico. Ogni azione aggressiva commessa sia da un attore statale sia da un attore non statale e diretta a colpire la sicurezza nazionale di un Paese

[10] KULESZA, BALLESTE (2015: 2).
[11] Convenzione del Consiglio d' Europa sulla criminalità informatica, Budapest, 23 novembre 2001, articoli 2, 4, 5, 6, 7, 8, 9, 10.
[12] Manuale delle Nazioni Unite sulla prevenzione e il controllo del crimine informatico del 1994.
[13] HATHAWAY, CROOTOF, LEVITZ, NIX, NOWLAN, PERDUE, SPIEGEL (2011: 7 ss.).

perciò, deve ritenersi un attacco informatico. Viceversa, qualsiasi azione che non persegua tale scopo, pensiamo alle frodi *on-line* o alla pirateria informatica, non rientra in tale definizione.
Soltanto in caso di *cyber attack*, inoltre, si prospetta l'idea di poter invocare il regime di responsabilità internazionale di uno Stato (laddove questo possa configurarsi come il vero responsabile dell'attacco), di cui parleremo nel prossimo capitolo.
In conclusione, in alcuni casi un *cyber attack* può contestualmente rappresentare anche un crimine informatico mentre non è possibile affermare il contrario: non tutti i *cyber crimes* sono anche dei *cyber attacks*.

Gli attacchi informatici sono comunemente divisi in due principali categorie: gli attacchi sintattici e gli attacchi semantici.

Gli attacchi sintattici

Quando parliamo di attacchi sintattici facciamo riferimento ad attacchi di tipo diretto indirizzati contro un preciso bersaglio, che puntano a neutralizzare o distruggere; essi vengono effettuati infettando i sistemi informatici oggetto di attacco attraverso *software* malevoli quali *virus*, *worms* o *Trojan Horses*[14].
I *virus* sono dei programmi auto-replicanti che possono essere legati ad altri file o programmi e che tendono a riprodursi in maniera incessante.
Le caratteristiche principali di un *virus* consistono nella sua capacità di nascondersi nelle zone più improbabili della memoria di un computer e in quella di infettare qualunque file adatto all'esecuzione del proprio codice; inoltre, esso riesce a modificare la propria impronta digitale ogni qualvolta si riproduce riducendo, così, le probabilità di essere individuato.
Gli *worms* funzionano come i *virus* e sono anch'essi dei programmi auto-replicanti; si differenziano da questi, tuttavia, poiché non necessitano di altri file o programmi in quanto programmi ad esecuzione autonoma. Essi scovano le vulnerabilità di un sistema per penetrarlo, eseguire il proprio codice e replicarsi in altri sistemi. Solitamente, il loro impiego avviene nell'ambito dello spionaggio industriale poiché sono in grado di analizzare, conservare e ritrasmettere a chi li ha creati le attività dei sistemi informativi oggetto di attacco.
I *Trojan Horses* sono, invece, utilizzati per lo più per raccogliere informazioni senza che un utente se ne accorga; in genere, l'attacco avviene mediante messaggi di posta elettronica, browser web, *software* per chat o *software* per il controllo remoto e gli aggiornamenti. In ogni caso, il bersaglio solitamente è un individuo o in linea di massima un'istituzione.

[14] ANTOLIN-JENKINS (2008: 140 ss.).

Gli attacchi semantici

Solitamente, questo tipo di attacchi consiste nella diffusione di false informazioni o richieste con lo scopo di coprire le proprie tracce e/o indirizzare il nemico verso una direzione sbagliata che egli, tuttavia, crederà essere quella giusta. Ciò accade perché il sistema oggetto di un attacco di tipo semantico sembrerà funzionare in maniera corretta sebbene esso generi, nei fatti, dati errati[15].
Un tipico attacco semantico è rappresentato dal c.d. attacco DDoS (*Distributed Denial-of-Service*).
Esso è una variante del DoS (*Denial-of-Service*), attacco mirato ad arrestare un computer o una rete per ostacolare il libero accesso agli utenti autorizzati che avviene inondando il bersaglio di dati o mediante l'invio di informazioni che generano un blocco dei sistemi. L'obiettivo è impedire agli utenti l'accesso ad un servizio o ad una risorsa.
Un attacco DDoS è molto simile ma più potente poiché in grado di coinvolgere un vastissimo numero di computer (che vengono infettati e fatti, involontariamente, partecipare all'attacco). Questa tipologia di attacco è molto diffusa: esaminiamo il seguente caso.

Il caso dell'Estonia

Il 27 aprile 2007 l'Estonia decise di rimuovere dalla capitale Tallin, e spostare verso un cimitero militare situato fuori dalla città, una statua di bronzo alta più di due metri raffigurante un soldato con l'uniforme dell'Armata Rossa morto durante la II guerra mondiale in seguito ad uno scontro con i nazisti, diventata simbolo della sua vecchia appartenenza all'URSS.
A quest'evento seguirono numerose proteste da parte dei cittadini estoni di origine russa, che presto sfociarono nella violenza e nell'arresto di diverse persone. A ciò si aggiunse una serie di attacchi DDoS contro numerosi siti web nazionali che furono resi inaccessibili; inoltre, si provocò la paralisi di tutte quelle sovrastrutture collegate alla rete (come il governo o le banche nazionali). La questione si risolse con l'intervento da parte della NATO e degli USA, i quali inviarono dei loro esperti nel Paese per investigare e proteggere i sistemi informatici da ulteriori minacce[16].
La vicenda estone fu di importanza fondamentale perché mostrò al mondo la vulnerabilità delle società contemporanee e le conseguenze di un attacco informatico.
Da allora, molti governi hanno preso coscienza dei pericoli che nasconde la rete e della minaccia che i *cyber attacks* rappresentano per la sicurezza e la stabilità di un Paese nonché per il benessere dei suoi cittadini.

[15] LIBICKI (1995: 77).
[16] WEISSBRODT (2017: 349-351).

Ad essere oggetto di attacchi informatici spesso sono soprattutto le cosiddette infrastrutture critiche di un Paese. Gas, elettricità, sistemi di difesa, servizi finanziari e molto altro oggi dipendono, nella gran parte dei casi, da computer connessi tra di loro e alla rete. Nell'ipotesi in cui queste siano oggetto di un attacco informatico, qualsiasi sia la sua entità, un Paese potrebbe trovarsi completamente paralizzato o veder minata la propria stabilità e la propria capacità di proteggere la sua popolazione.
Esistono anche altre tipologie di attacchi semantici.
La più nota prevede la disseminazione di informazioni inaccurate in un sistema informatico. Il fine ultimo che si persegue varia da caso a caso; generalmente, si punta a compromettere i sistemi informatici oggetto dell'attacco in modo da impedire l'accesso ad informazioni reali e corrette.
Per capire meglio di cosa stiamo parlando, è utile portare all'attenzione due casi realmente accaduti.

Il caso degli Stati Uniti

Il primo di essi riguarda gli Stati Uniti, che nel 1999 elaborarono un piano per diffondere dati falsi all'interno del sistema informatico del comando di difesa aerea della Serbia, al fine di impedire a quest'ultima di intercettare i velivoli della NATO[17] (in quel periodo impegnati in una campagna di bombardamenti contro il regime serbo di Slobodan Milošević).
Il piano non fu, in seguito, attuato a causa di alcuni problemi legali riguardanti i danni collaterali che un tale attacco avrebbe prodotto.
Se consideriamo, però, l'ipotesi in cui tale piano avesse visto la luce probabilmente la Serbia non sarebbe stata in grado di difendersi in maniera adeguata poiché non avrebbe avuto le capacità di rilevare la presenza di velivoli in volo nel proprio spazio aereo pronti ad attaccare.
Appare evidente, allora, quanto un simile attacco informatico possa risultare decisivo in un conflitto e in grado di far spostare le lancette in favore dell'una o dell'altra parte; infatti, con facilità si riuscirebbe a sorprendere l'avversario, ignaro rispetto a ciò che sta accadendo.

Il caso siriano

Una strategia molto simile è stata messa in atto da Israele nel 2007, durante i bombardamenti aerei organizzati dal Paese contro una struttura nucleare siriana. Di fatto, i velivoli israeliani riuscirono non soltanto ad invadere lo spazio aereo siriano senza incontrare alcun ostacolo ma anche a colpire esattamente l'obiettivo a seguito di un attacco al sistema di difesa aereo siriano. Non sono note le modalità precise dell'attacco: si ipotizza che Israele abbia inviato falsi messaggi ai radar siriani che non hanno, così,

[17] ARKIN (1999: 1 ss.).

intercettato la presenza di alcun velivolo[18] e che, perciò, hanno impedito una risposta difensiva.
Questo prova le potenzialità di un attacco informatico di tale genere, in grado di consentire a chi lo mette in atto di agire indisturbato e a chi ne è vittima di non accorgersi di ciò che sta avvenendo se non, spesso, troppo tardi e cioè una volta che chi ha perpetrato l'attacco ha raggiunto il proprio scopo.

[18] CLARKE, KNAKE, (2010: 1-9).

1.2 Le infrastrutture critiche come bersaglio

Come precedentemente delineato, con sempre più frequenza, le infrastrutture critiche di un Paese sono bersaglio di attacchi informatici.
Per infrastruttura critica si intende generalmente un sistema o una risorsa la cui distruzione, interruzione o momentanea indisponibilità indebolisce in maniera significativa l'efficienza o il normale funzionamento di un Paese.
Solitamente sono associati al concetto di infrastrutture critiche le risorse idriche, il sistema di telecomunicazioni, i trasporti, le banche e i servizi finanziari o la sanità.
Esaminiamo alcune tra le più diffuse definizioni di infrastruttura critica.
A livello europeo, l'8 dicembre 2008 il Consiglio dell'Unione europea ha emanato la direttiva 2008/114/CE *relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione* che al punto a) dell'art. 2 sancisce che un'infrastruttura critica consiste in un:

> asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

Nello stesso modo ha proceduto lo U.S. Homeland Security Office, il quale descrive un'infrastruttura critica come l'insieme di :

> assets, systems and networks, both physical and digital, which are so important to the state that their incapacitation or destruction would have debilitating effect on security, national economic security, national public health or safety, or any combination thereof[19].

Infine, molto importante è la definizione fornita dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) che considera infrastrutture critiche i seguenti settori: "energy, transportation, telecommunications and information systems"[20].
Tale organizzazione, con riferimento alla protezione delle infrastrutture critiche, non prende in considerazione la natura delle potenziali minacce contro di esse; adotta, piuttosto, un approccio che comprende una pluralità di casistiche (dai disastri naturali ai *cyber crimes*): di fatti, nella 'Raccomandazione sulla governance dei rischi maggiori', si afferma che eventuali minacce o pericoli possono originare da diversi eventi, fra i quali per l'appunto "earthquakes, industrial accidents, terrorist attacks, pandemics,

[19] U.S. Office of Homeland Security, *What Is Critical Infrastructure?*, 2013, reperibile *on-line*.
[20] Raccomandazione dell'Organizzazione per la Cooperazione e lo Sviluppo Economico del 6 maggio 2014, *sulla governance dei rischi maggiori*.

illicit trade or organized crime"[21]. Si raccomanda inoltre, al fine di assicurare la loro protezione, la partecipazione tanto del governo quanto del mondo privato e dei singoli individui.
L'approccio proposto dall'OCSE propone di realizzare la tanto discussa *Public-Private Partnership*: un modello di collaborazione tra i vari livelli di governo con lo scopo di elaborare congiuntamente politiche di sicurezza delle infrastrutture critiche.
Il modello di *partnership* offerto dal documento dell'OCSE rappresenta l'attuale tendenza nell'ambito della *cyber security*, nel quale forte è l'enfasi posta sulla necessità di un coinvolgimento del settore privato e di una cooperazione multilivello per affrontare quelle che sono oggigiorno le minacce alla sicurezza di un Paese.
Certamente non tutte le infrastrutture critiche sono collegate ad una rete ma, laddove ciò avviene, emerge l'esigenza di garantire la protezione degli *assets* e dei dati che si utilizzano e di prevenire l'intrusione non autorizzata in questi sistemi o la diffusione di informazioni sensibli. Ed è soprattutto a partire dagli anni 2000, come riferisce un rapporto sui problemi della sicurezza in ambito industriale, redatto dal British Columbia Institute of Technology e dal PA Consulting Group, che si è riscontrato un aumento di 10 volte nel numero dei successi di attacchi informatici alle infrastrutture con sistemi di controllo SCADA (*Supervisory Control And Data Acquisition*, sistema informatico distribuito per il monitoraggio elettronico di sistemi fisici) e si è ravvisata l'emergenza di adottare tutte le misure necessarie ad affrontare simili attacchi.

Il caso STUXNET

Il caso del virus STUXNET è uno dei più noti casi di attacco informatico ai sistemi SCADA. Questo virus informatico era stato appositamente creato dal governo statunitense, come la stessa amministrazione del Presidente degli Stati Uniti Barack Obama nel 2012 ha confermato[22], in collaborazione con il governo israeliano e nell'ambito dell'operazione '*Olympic Games*' (promossa da Bush nel 2006 e attuata da Obama) che prevedeva la messa in atto di una serie di attacchi informatici contro l'Iran. Lo scopo dell'operazione era distruggere il programma nucleare iraniano.
Più precisamente, STUXNET era stato creato per modificare l'andamento delle centrifughe della centrale nucleare iraniana di Natanz utilizzate per separare i materiali nucleari come l'uranio arricchito[23] in modo da impedire il corretto sviluppo di tale operazione senza che, tuttavia, venissero rilevati dai sistemi malfunzionamenti e, ovviamente, la presenza di tale virus.

[21] *Ibidem.*
[22] SANGER, *Obama Order Sped up Wave of Cyber attacks Against Iran*, in *The New York Times*, 1 giugno 2012, reperibile *on-line*.
[23] KUSHNER (2014: 1 ss.).

A seguito di alcune indagini, è emerso che il contagio si sia prodotto probabilmente a partire da una chiavetta USB infetta di uno degli impiegati dello stabilimento, forse ignaro. Da quel momento in poi, il virus è riuscito a diffondersi via rete a tutto il sistema informatico della centrale. Il virus ha ottenuto i risultati che erano stati prefissati riuscendo, contemporaneamente, a far credere che tutto funzionasse correttamente. Questo, fintanto che, a causa di un errore di programmazione presente nel virus stesso, non si è verificata la sua diffusione al di fuori dello stabilimento nucleare tramite il PC casualmente infettato di un ingegnere. A quel punto, STUXNET, non soltanto è stato scoperto dagli iraniani, ma è finito anche sotto l'attenzione dei media di tutto il mondo.
Ciò detto, gli aspetti rilevanti dell'intera vicenda sono almeno due: da un lato, la sofisticazione del *software* STUXNET dimostra che chi ha creato tale programma conosceva molto bene i sistemi informativi della centrale nucleare e come questi funzionavano; dall'altro, il successo dell'attacco, seppur per un breve periodo, ha dimostrato che è possibile compromettere un sistema a tal punto da rendere difficile tanto l'individuazione del virus quanto le sue conseguenze, nel caso specifico il malfunzionamento delle centrifughe.
Infine, è d'obbligo sottolineare come sia stato facile per i responsabili infettare i sistemi informativi della centrale attraverso un dispositivo oggi comunemente impiegato dagli individui (vale a dire una chiavetta USB), poco consapevoli delle criticità e vulnerabilità legati al mondo dell'informatica.

Le infrastrutture più a rischio

Ad essere minacciati da eventuali attacchi *cyber* sono soprattutto i sistemi di controllo, i settori dell'energia, delle telecomunicazioni, dei trasporti, idrico e della finanza. Si tratta, infatti, di settori di importanza fondamentale per il buon funzionamento di un Paese e per la sua stabilità.
Consideriamone le ragioni.
I sistemi di controllo responsabili dell'attivazione e del monitoraggio industriale o dei controlli meccanici sono spesso dei bersagli per i criminali informatici, cosiddetti *hackers*, in quanto, scovate le loro vulnerabilità, è semplice ottenere informazioni rilevanti e prendere il controllo di interi impianti. Infatti, tali sistemi sono progettati solitamente per rilevare tutti i dispositivi dotati di connessione utilizzati all'interno di un impianto e, di conseguenza, per gestirli. Se si riuscisse a penetrare tali sistemi, abbattendo eventuali meccanismi di protezione, risulterebbe molto semplice monitorare tutti i dispositivi dipendenti da questi e acquisirne il controllo.
Per quanto riguarda il settore dell'energia, invece, qui la situazione riguarda soprattutto due fonti energetiche considerate strategiche: l'elettricità e il gas naturale.
L'una alimenta imprese, abitazioni e locali di vario genere in tutto il territorio di uno Stato; l'altra può, in caso di attacco, essere interrotta o

ridirezionata verso altri impianti e causare perdite ingenti al Paese o ai Paesi che ne necessitano o che, al contrario, la distribuiscono. Ciò detto, qualsiasi sia la fonte energetica colpita le conseguenze di un attacco informatico sono le medesime: si va dall'isteria di massa, all'aumento della domanda energetica fino ad arrivare al caos e all'instabilità interna e/o internazionale.
Emblematico è stato il caso dell'azienda russa fornitrice di gas 'Gazprom' che, nel 1999, vide alcuni *hackers* riuscire a *bypassare* i controlli di sicurezza e ad introdurre nei sistemi informatici dell'azienda un *Trojan Horse*, a causa del quale Gazprom perse, per un certo periodo di tempo, il controllo del suo centralino principale che regolava il flusso di gas.
Attacchi ancor più pericolosi e con i risultati immediati sono quelli a danno dei settori delle telecomunicazioni e dei trasporti.
Per ciò che riguarda l'ambito delle telecomunicazioni, un attacco informatico può essere perpetrato con lo scopo di interrompere il flusso di comunicazioni tra più soggetti e provocare, dunque, un isolamento della o delle vittime. Poniamo l'ipotesi di un conflitto armato: attraverso un simile attacco si riuscirebbe a prendere il sopravvento sul nemico più facilmente poiché si minerebbe la sua capacità di scambiare informazioni e organizzare una propria difesa. Le comunicazioni sono, infatti, di importanza fondamentale per venire a conoscenza di un attacco e per dispiegare le proprie forze in funzione difensiva o in funzione ausiliare rispetto ad un un'unità militare in difficoltà. Se queste vengono tagliate, le conseguenze sono facilmente intuibili. Non solo. Il fine ultimo degli *hackers*, anche nel settore delle telecomunicazioni, può essere di tipo economico. Come è accaduto al colosso delle telecomunicazioni spagnolo 'Telefonica'[24], ad un attacco informatico può seguire la richiesta di un riscatto in cambio della cessazione di ogni azione intrusiva, del ripristino dello *status quo ante* e della riabilitazione all'uso di tutti i sistemi informativi.
Con riferimento al settore dei trasporti, invece, un *cyber attack* può essere in grado di danneggiare i sistemi ferroviari, le strade ed impedire così il trasporto convenzionale o addirittura colpire i sistemi di volo e provocare l'interruzione del normale traffico aereo e/o gravi incidenti. Tutto ciò procurerebbe danni economici e non di certo rilevanti.
Tra le infrastrutture più a rischio vi è anche il sistema idrico. Tutti quegli impianti idrici informatizzati sono spesso oggetto di attacchi informatici in quanto, laddove si riuscisse ad acquisirne il controllo, si avrebbe la possibilità di rilasciare enormi quantità d'acqua su zone non protette e provocare danni strutturali gravissimi, se non anche la perdita di vite umane.

[24] "I gruppi spagnoli delle TLC Telefonica e Tuenti sono stati oggetto in mattinata di un massiccio attacco informatico[…]. Ai dipendenti della sede Telefonica di Madrid la cui Rete interna è stata colpita, è stato ordinato, anche attraverso megafoni, di spegnere tutti i computer e i dispositivi elettronici. In un classico schema di attacco informatico il *malware* […] avrebbe criptato i file memorizzati sugli hard disk chiedendo un riscatto in *bitcoin* per renderli nuovamente accessibili da pagare entro il 15 maggio. L'importo chiesto sarebbe equivalente a 300 dollari", Mauro Del Corno, *Telefonica e Tuenti vittime di attacco informatico, chiesto riscatto, Il Sole 24 ore*, 12 maggio 2017, reperibile *on-line.*

Ad essere oggetto di attacchi è, talvolta, persino il sistema fognario, il cui mal funzionamento potrebbe provocare allagamenti, cattivo smaltimento dei rifiuti o inquinamento delle acque.

Con riferimento al settore finanziario, l'obiettivo di un *cyber attack* può essere quello di rubare grandi somme di denaro o di interrompere anche solo per un giorno il flusso di denaro causando danni permanenti agli investitori ed erodendo la fiducia del pubblico. Non soltanto. Spesso i criminali informatici puntano a ricattare una banca rubando i dati personali dei suoi clienti o a demolirne la credibilità e la reputazione rendendo pubblici tali dati. Per capire la gravità di queste azioni analizziamo due casi divenuti di grande interesse.

Attacco informatico alla banca centrale del Bangladesh

Il primo caso riguarda la banca centrale del Bangladesh che, nel febbraio 2016, è stata vittima di un attacco da parte di alcuni *hackers*. Questi, sono riusciti a rubare 81 milioni di dollari.
La banca in questione aveva un miliardo di dollari di riserve in seno ad un conto bancario della Federal Reserve degli Stati Uniti e si ritiene che l'obiettivo iniziale consistesse nel sottrarre l'intera somma. In ogni caso, la somma prelevata non è stata irrisoria.
L'operazione ha avuto luogo nel seguente modo: i responsabili dell'attacco dapprima hanno compromesso il sistema informativo della banca centrale per osservare le modalità di trasferimento del denaro; in un secondo momento, sono riusciti ad accedere alle credenziali della banca necessarie per eseguire le diverse transazioni e, infine, hanno utilizzato tali credenziali per autorizzare tre dozzine di richieste alla Federal Reserve relative al trasferimento di fondi dall'account della banca centrale del Bangladesh ad account di alcune fondazioni che si trovavano nello Sri Lanka e nelle Filippine.
L'incidente ha mostrato, ancora una volta, i rischi connessi al mondo *cyber* e ha segnato il punto di partenza, non soltanto per il Bangladesh ma anche per altri Paesi, verso nuove politiche di sicurezza informatica.

Il caso della JP Morgan Chase & Co

Il secondo caso che consideriamo riguarda la JP Morgan Chase & Co, società americana leader nei servizi finanziari.
Nel 2014 la società è stata vittima di un attacco informatico che ha permesso ad un gruppo di *hackers* la sottrazione dei dati personali di oltre 83 milioni di account[25]. Sebbene né codici di sicurezza né password siano stati compromessi, la banca ha dichiarato che nomi, indirizzi mail, indirizzi

[25] BERNARD, *Ways to Protect Yourself After the JPMorgan Hacking*, in *The New York Times*, 4 ottobre 2014, reperibile *on-line*.

postali e numeri di telefono sono finiti nelle mani dei criminali informatici e che, pertanto, i clienti della banca sarebbero dovuti rimanere in uno stato di allerta per evitare di essere vittima di ulteriori crimini.
Questo episodio è considerato come una delle intrusioni più gravi avvenute all'interno di un'azienda americana e uno dei più ingenti furti di dati nella storia[26].

A questo punto, è chiara la necessità di elaborare strategie di *cyber defence* tanto a livello nazionale quanto a livello internazionale.
Nei prossimi paragrafi esamineremo le politiche in ambito *cyber* intraprese, nello specifico, dall'Unione europea e dall'Italia per scoprire quale approccio è stato seguito fino ad oggi nel contesto europeo.

[26] MUNOZ, *JP Morgan hack exposed data of 83 million, among biggest breaches in history*, 3 ottobre 2014, in *REUTERS*, reperibile *on-line*.
GOLDSTEIN, PERLROTH, SANGER, *Hackers' Attack Cracked 10 Financial Firms in Major Assault*, in *The New York Times*, 04 aprile 2014, reperibile *on-line*.

1.3 La strategia dell'Unione europea in materia di *cyber defence*

L'Unione europea ha iniziato a concentrare la propria attenzione sulla necessità di attuare politiche di *cyber security* negli anni Duemila. Inizialmente, fra l'altro, all'interno dei primi documenti europei approvati, relativi all'individuazione delle priorità in materia di sicurezza delle reti, non veniva mai utilizzato il termine '*cyber security*'. Per questo, dovremo attendere il 2008. Fino a quel momento, l'Unione europea si occuperà soprattutto di *cyber crimes* e protezione delle infrastrutture critiche.
Il primo passo viene compiuto proprio nel 2000, quando la Commissione europea elabora una comunicazione sul *cyber crime*[27] nella quale si esaminano due questioni fondamentali:

1. la sicurezza delle infrastrutture dell'informazione;
2. la lotta al crimine informatico.

Tali, saranno le questioni sulle quali inizialmente l'Unione europea si concentrerà circa il perseguimento di un buon livello di sicurezza informatica.
L'anno successivo è un anno altrettanto importante: nel mese di giugno, la Commissione europea presenta un documento (dal titolo "*Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo"*) esclusivamente dedicato alla definizione di una politica strettamente europea di sicurezza informatica. Questo è il momento in cui l'Unione europea esplicita la propria volontà di intraprendere una sua strada in questo settore.
All'interno del documento troviamo una descrizione di quella che viene chiamata *Network and Information Security* (NIS), intesa 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[28].

Segue la definizione di un quadro di minacce alla sicurezza che potrebbero avere un impatto negativo sulla cosiddetta NIS, fra le quali troviamo:

- l'intercettazione delle comunicazioni;
- l'accesso non autorizzato a computer e reti informatiche;

[27] Comunicazione della Commissione europea del 26 gennaio 2001, COM(2000)890, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica*.
[28] Comunicazione della Commissione europea del 6 giugno 2001, COM(2001)298, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*.

- ‘la caduta della rete’; con tale espressione si vuol far riferimento a quegli attacchi informatici che provocano un’interruzione delle funzioni di un’infrastruttura, noti anche come ‘*disruptive attacks*’;
- l’esecuzione di *software* maligni che modificano o distruggono i dati all’interno di un sistema informatico;
- l’usurpazione di identità;
- gli incidenti ambientali e gli eventi imprevisti, dovuti a catastrofi naturali o incidenti provocati dall’errore umano[29].

In questi anni, vengono resi noti anche altri due documenti molto importanti: il documento del 2000 ‘eEurope’[30] e quello del 2002 ‘eEurope 2005’[31].
Il primo di questi è finalizzato alla promozione della digitalizzazione del mondo. I principali obiettivi dell’iniziativa ivi contenuta sono:

I. fare in modo che ciascun cittadino, ciascuna abitazione, scuola, impresa e amministrazione si integri a pieno nell'era digitale e disponga di un collegamento *on-line*;
II. favorire la padronanza degli strumenti dell'era digitale, anche grazie al sostegno di una cultura imprenditoriale pronta a finanziare e a sviluppare nuove idee;
III. garantire che l'intero processo non crei emarginazione, ma rafforzi la fiducia dei consumatori e potenzi la coesione sociale[32].

Per conseguire tali obiettivi la Commissione propone dieci azioni prioritarie, da attuare grazie all'impegno congiunto della Commissione stessa, degli Stati membri, dell'industria e dei cittadini europei. Fra queste ricordiamo la garanzia di un accesso più economico ad Internet e la fornitura di servizi sanitari o relativi alla Pubblica Amministrazione *on-line*.
Nel 2002 si decide di ampliare l’iniziativa, mediante ‘eEurope 2005’, al fine di garantire un accesso ad Internet più rapido ed economico, un maggior collegamento con le scuole per fornire loro servizi multimediali, formare gli insegnanti sulle tecnologie digitali e introdurre nuovi metodi di apprendimento attraverso l’uso di queste ultime; infine, si cerca di stimolare l’impiego di Internet, pur continuando contemporaneamente ad attuare misure che tutelino la sicurezza delle reti e degli utenti che vi operano.
Sempre nel 2002, vengono approvate tre importanti direttive in materia di *Network and Information Security.*

[29] CENCETTI (2014: 22 ss.).
[30] Comunicazione della Commissione europea dell’ 8 marzo 2000, COM(2000)130, *eEurope. Una società dell’informazione per tutti*.
[31] Comunicazione della Commissione europea del 28 maggio 2002, COM(2000)263, *eEurope 2005: una società dell’informazione per tutti*.
[32] Comunicazione della Commissione europea dell’ 8 marzo 2000, COM(2000)130, *eEurope. Una società dell’informazione per tutti*.

La prima è la direttiva 2002/21/CE, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica.
La seconda è la direttiva 2002/19/CE, relativa all'accesso alle reti di comunicazione elettronica nonché alle risorse correlate e all'interconnessione delle medesime.
Infine, la terza è la direttiva 2002/20/CE, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica.
Tutte e tre le direttive saranno abrogate nel 2009 (questo però lo vedremo più avanti).
Arriviamo al 2003, anno in cui l'Unione europea elabora, finalmente, una propria strategia, tutt'ora in vigore, in materia di sicurezza individuando nelle reti informatiche la sua vulnerabilità più grande.
Essa invita gli Stati membri a prendere, il prima possibile, tutte le misure necessarie ad armonizzare le loro politiche in materia di *cyber security*.
Sarà proprio in una delle relazioni sullo stato di implementazione a livello nazionale di tale strategia, e in particolare nella relazione del 2008, che verrà impiegato per la prima volta il termine '*cyber security*'.
Un altro anno molto importante è il 2004: in tale anno, viene approvato il regolamento (CE) 460/2004 che istituisce l'Agenzia europea di sicurezza delle reti e dell'informazione, meglio conosciuta con l'acronimo inglese ENISA - *European Network and Information Security Agency*. Essa ha prevalentemente il compito di assistere la Commissione e gli Stati membri nella loro missione di 'prevenzione e reazione' ai problemi di *cyber security*.
L'ENISA svolge, altresì, un ruolo di consulenza e contribuisce così ad incrementare il livello generale di competenze in ambito *cyber*. Infine, essa promuove e diffonde una nuova cultura della sicurezza incentrata sulla *cyber security*, di modo che questa venga presa in considerazione non soltanto a livello europeo ma anche a livello nazionale e che si inizi immediatamente a pensare, mediante gli opportuni strumenti legali, a come affrontare la minaccia proveniente dal *cyber* spazio.
Nello specifico, l'Agenzia coordina l'operato degli Stati membri e favorisce il dialogo fra questi; essa, inoltre, elabora linee guida, individua delle cosiddette *best practices* (regole di condotta) e pubblica numerosi documenti, liberamente consultabili *on-line*, per cercare di stimolare il confronto tra gli Stati e provvedere ad un monitoraggio e un aggiornamento continuo della situazione.
L'operato dell'agenzia è estremamente importante per quanto riguarda la promozione della cooperazione nell'ambito della *cyber security* e, a questo scopo, è stato istituito un meccanismo di *incident reporting*, per incentivare gli *Internet and Service Provider* (ISP) a rendere pubblici gli attacchi cibernetici subiti. Tale meccanismo prevede, allo stesso tempo, il coinvolgimento delle autorità nazionali competenti e delle istituzioni europee interessate.
Esso consiste, di fatto, in un vasto sistema di notificazione e scambio di informazioni tra tutti gli attori coinvolti: i *provider*, gli utenti, le autorità nazionali competenti, l'ENISA e la Commissione. Più specificamente, spetta

a queste ultime due adottare le misure di sicurezza opportune ed indirizzarle verso le autorità nazionali competenti ed i *provider*[33].
Come è osservabile, dunque, le strutture europee vengono poste al vertice di questa architettura, cosicché le azioni siano coordinate a livello sovranazionale.
Tuttavia, la realtà è ben diversa dalle aspettative. Infatti, spesso non viene data comunicazione della verifica di attacchi informatici: le imprese, ma anche gli Stati stessi, preferiscono tacere a riguardo piuttosto che rivelare di avere falle nel proprio sistema e veder danneggiata la propria reputazione. Qui sta forse l'impresa più ardua che l'ENISA dovrà affrontare nei prossimi anni e cioè promuovere un cambiamento a livello di approccio alle questioni di *cyber security*: si dovrà puntare alla trasparenza e alla condivisione.
Con un breve salto temporale giungiamo al 2006, anno in cui la Commissione elabora la comunicazione relativa a una strategia per una 'società dell'informazione sicura'[34], nella quale nuovamente si riporta all'attenzione il bisogno di impegnarsi nella diffusione di una maggiore sicurezza delle reti e delle informazioni e di una cultura della *cyber security*.
Nello stesso anno viene approvata anche la comunicazione della Commissione relativa ad un programma europeo per la protezione delle infrastrutture critiche[35], mediante la quale viene istituito il CIIP (*Critical Information Infrastructure Protection*) per favorire il coordinamento e la cooperazione tra gli Stati ai fini del perseguimento del programma europeo.
Il CIIP è presieduto dalla Commissione e riunisce tutti i punti di contatto PIC (Protezione infrastrutture critiche) nazionali. Esso assiste gli Stati membri aiutandoli ad individuare le infrastrutture nazionali più critiche sulla base di due criteri: la portata, cioè l'ampiezza dell'area geografica che potrebbe subire danni in seguito ad un attacco e la gravità, che prende in considerazione le conseguenze di una neutralizzazione o distruzione di un'infrastruttura critica. Nello specifico, si prendono in considerazione gli effetti a livello economico, politico, ambientale, psicologico, di salute pubblica e, infine, si prende eventualmente in considerazione il numero di persone colpite.
Il programma europeo dedicato alla protezione delle infrastrutture critiche continuerà ad essere sviluppato anche negli anni successivi a tale comunicazione che ha, però, certamente segnato il punto di partenza della strategia europea in quest'ambito.
Arriviamo al 2008, anno in cui viene per la prima volta impiegato il termine *cyber security* in ambito europeo e in cui viene anche approvata la direttiva 2008/114/CE del Consiglio dell'Unione europea relativa all'individuazione e

[33] CENCETTI (2012: 115 ss.).
[34] Comunicazione della Commissione europea del 31 maggio 2006, COM(2006)251, *Una strategia per una società dell'informazione sicura. Dialogo, partenariato e responsabilizzazione*.
[35] Comunicazione della Commissione europea del 12 dicembre 2006, COM(2006)786, *Comunicazione relativa a un programma europeo per la protezione delle infrastrutture critiche.*

alla designazione delle infrastrutture europee (cosiddette ECI, *European Critical Infrastructure*), che avvengono sulla base di taluni criteri volti a definire il peso e l'importanza effettivi di un'infrastruttura e alla valutazione della necessità di migliorarne la protezione.
In base a tale direttiva, viene definita ECI ogni infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri[36].
Procedendo con l'esame dei documenti europei più importanti in ambito *cyber* esaminiamo quelli risalenti al 2009.
Parliamo, innanzitutto, della cosiddetta 'direttiva *framework*', ossia la direttiva 2009/140/CE recante modifica delle direttive 2002/21/CE, 2002/19/CE e 2002/20/CE.
Essa è importante soprattutto perché obbliga gli Stati membri dell'Unione europea ad istituire una serie di autorità nazionali di regolamentazione per quanto riguarda la sicurezza delle reti.
In secondo luogo, rilevante è anche la comunicazione presentata dalla Commissione europea relativa alla protezione delle infrastrutture critiche informatizzate. In questa comunicazione, viene messa in evidenza la necessità di proteggere tali infrastrutture, vitali per la crescita di un Paese, e viene definito un piano d'azione volto a rafforzare la loro sicurezza e la loro resilienza. A riguardo, un ruolo speciale viene riservato all'ENISA, soprattutto nell'ambito della prevenzione, nel quale contribuisce realizzando un forte coordinamento delle politiche dei vari Stati membri.
Anche nel 2010 vengono pubblicati alcuni documenti interessanti.
Il primo consiste nell'Agenda digitale europea, finalizzata ad ottenere vantaggi socioeconomici sostenibili grazie a un mercato digitale unico basato su Internet veloce e superveloce e su applicazioni interoperabili[37].
Perché creare un mercato digitale unico? Da una parte, in tal modo si acquisisce una maggiore capacità di incrementare la sicurezza dei cittadini europei; dall'altra, si diventa in grado di attrarre un numero sempre maggiore di investimenti, a beneficio della domanda e dell'offerta.
Il secondo documento è relativo alla strategia di sicurezza interna dell'Unione europea. In esso si tenta di meglio definire quali siano le minacce alla sicurezza europea e la strade da seguire per ridurre il loro impatto.
Nello specifico, si invitano gli Stati a mettere in atto le seguenti azioni:

a) smantellare le reti criminali internazionali;
b) prevenire il terrorismo e contrastare la radicalizzazione e il reclutamento;

[36] Direttiva (UE) del Consiglio dell'8 dicembre 2008, 2008/114, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.
[37] Comunicazione della Commissione europea del 26 agosto 2010, COM(2010)245, *Un'agenda digitale europea*.

c) aumentare i livelli di sicurezza per i cittadini e le imprese nel *cyber* spazio:
d) rafforzare la sicurezza attraverso la gestione delle frontiere;
e) aumentare la resilienza dell'Europa alle crisi e alle calamità[38].

Per garantire la realizzazione di questo progetto, soprattutto per quanto riguarda il punto c), l'Unione europea stabilisce tre linee d'azione.
La prima prevede la creazione di un Centro europeo per il *cyber crime*, che sarà istituito già nel 2012 per diventare operativo l'anno successivo.
La seconda mira a sviluppare un meccanismo di *incident reporting* mediante il quale cittadini e imprese possono informare chi di dovere relativamente al verificarsi di attacchi informatici.
La terza consiste nella messa in atto di una cooperazione tra CERT (*Computer Emergency Response Team*, ovvero un'organizzazione incaricata di raccogliere le segnalazioni da parte della comunità degli utenti relative a incidenti informatici o all'individuazione di potenziali vulnerabilità nei sistemi) nazionali e CERT-EU finalizzata alla creazione di un sistema europeo di condivisione delle informazioni e di allarme.
Il vero e proprio anno di svolta, tuttavia, sarà il 2013: il 7 febbraio, infatti, viene approvato il primo documento strategico globale in materia di *cyber security* che si intitola '*An Open, Safe and Secure Cyber space*', al quale lavorano sia la Commissione sia l'Alto Rappresentante per gli affari esteri e la politica di sicurezza.
In esso, si porta all'attenzione la questione relativa alla dipendenza del mondo contemporaneo nei confronti dei sistemi digitalizzati e si attesta che, se da un lato, questi hanno migliorato la qualità della vita, dall'altro costituiscono una fonte permanente di rischi.
Lo scopo che l'Unione europea si prefigge è, allora, quello di garantire l'esistenza di uno spazio cibernetico 'aperto e sicuro'. Dunque, i medesimi valori che hanno segnato il processo di integrazione europea si ritiene debbano essere applicati anche nel *cyber space*, ove libertà e protezione saranno i principi cardine (nello specifico, parliamo di protezione dei diritti fondamentali, dei dati personali e della *privacy*; necessità di consentire un accesso senza limitazioni a tutti i cittadini, realizzazione di una governance condivisa tra attori pubblici e privati nella gestione della rete e, infine, rispetto dello stato di diritto e della democrazia).
La tutela e il rispetto di tutti questi valori rappresenta una *conditio sine qua non* per il raggiungimento dei vari obiettivi che l'Unione europea vuole raggiungere, fra i quali:

- conseguire la resilienza informatica;
- ridurre drasticamente la criminalità informatica;

[38] Comunicazione della Commissione europea del 22 novembre 2010, COM(2010)673, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*.

- sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune (CSDP);
- sviluppare le risorse industriali e tecnologiche per la sicurezza
- informatica;
- istituire una coerente politica del *cyber* spazio per l'Unione europea e sostenere i valori fondamentali della stessa[39].

Al fine di attuare, poi, un efficace coordinamento con gli Stati e una cooperazione tra il settore pubblico e il settore privato, l'Unione europea invita questi a sviluppare delle proprie strategie nazionali di *cyber security* in linea con i dettami europei.
Questo documento getta, senza alcun dubbio, le basi per una futura politica di sicurezza informatica europea ed è certamente fondamentale poiché enuncia i cosiddetti *core values* e le *good practices* che dovranno essere rispettati e promossi in materia. Il percorso verso uno spazio cibernetico aperto e sicuro è però ancora lungo.

Per quanto riguarda, invece, gli ultimi sviluppi a livello europeo in tema di *cyber security* rilevante è la cosiddetta 'direttiva NIS', adottata dal Parlamento europeo nel luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea. Questa direttiva può essere inquadrata all'interno della strategia europea di cui abbiamo parlato precedentemente.
Essa nasce con l'obiettivo di definire disposizioni minime in materia di pianificazione, scambio di informazione, cooperazione e obblighi di sicurezza comuni a tutti gli Stati membri dell'Unione, in particolare agli operatori di servizi essenziali e ai fornitori di servizi digitali che ivi operano.
La direttiva è entrata in vigore nell'agosto 2016 e stabilisce un periodo di tempo pari a due anni, entro i quali gli Stati dovranno recepire il suo contenuto all'interno del proprio ordinamento nazionale. Ad ogni modo, fermo restando il livello di armonizzazione previsto dall'Unione europea, questi sono liberi di adottare anche norme che garantiscano una maggiore protezione.
Esaminiamo nel dettaglio la direttiva. Cerchiamo di capire, innanzitutto, chi siano i destinatari della stessa: i fornitori di servizi digitali e gli operatori di servizi essenziali.
Con la prima espressione si indica qualsiasi persona giuridica che offra un servizio digitale, così come inteso nella direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione e nella stessa direttiva NIS

[39] Documento della Commissione europea, del 7 febbraio 2013, JOIN, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber space*.

che, a riguardo, riporta un elenco dei servizi digitali di riferimento: *on-line marketplace*, motori di ricerca *on-line*, *cloud computing*[40].
Relativamente agli operatori di servizi essenziali, la direttiva non opera un'identificazione diretta ma fornisce soltanto alcuni criteri per la loro individuazione. In particolare, è tale il soggetto pubblico o privato, facente parte delle categorie di settori elencate nell'allegato 2 della medesima direttiva (energia, trasporti, settore bancario, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, infrastrutture dei mercati finanziari), che soddisfa i seguenti criteri:

- deve trattarsi di un soggetto che fornisce un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
- la fornitura di tale servizio deve dipendere dalla rete e dai sistemi informativi;
- il verificarsi di un incidente deve, nel caso, avere effetti negativi rilevanti sulla fornitura di tale servizio[41].

Per quanto riguarda il contenuto della direttiva, essa prevede una serie di azioni finalizzate ad incrementare il livello di sicurezza delle reti e dei sistemi informativi in tutta l'Unione europea. Nello specifico:

1. si invitano gli Stati membri a munirsi di strumenti appropriati ad affrontare la minaccia cibernetica;
2. si chiede agli Stati membri di cooperare tra loro, anche mediante l'istituzione un gruppo di cooperazione composto da rappresentanti degli Stati membri, dalla Commissione e dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), al fine facilitare lo scambio di informazioni e accrescere la fiducia reciproca. Essi dovranno anche creare una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (rete CSIRT) allo scopo di promuovere una cooperazione operativa rapida ed efficace su specifici incidenti e condividere le informazioni relative ai rischi;
3. si promuove lo sviluppo della cultura della sicurezza nei settori che sono vitali per l'economia e la società, e che si basano profondamente sulle tecnologie dell'informazione e della comunicazione.
   I soggetti pubblici e privati che operano in questi settori e che saranno individuati dagli Stati membri come operatori di servizi essenziali dovranno prendere, allora, le appropriate misure di sicurezza per prevenire e minimizzare l'impatto di eventuali incidenti, al fine di assicurare la continuità di tali servizi; dovranno,

[40] VICARELLI, *La direttiva NIS: il primo passo della strategia europea per la cyber security*, 16 febbraio 2017, in *Diritto informatico*, reperibile *on-line*.
[41] *Ibidem*.

inoltre, notificare gli incidenti rilevanti all'autorità nazionale competente.
Anche i fornitori di servizi digitali dovranno conformarsi ai requisiti di sicurezza e al regime delle notifiche previsti dalla direttiva. Precisiamo che la direttiva NIS definisce incidente 'ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi'[42].

Gli operatori di servizi essenziali e i fornitori di servizi digitali sono tenuti, allora, a notificare all'autorità competente o al CSIRT ogni incidente che abbia:

1. un impatto rilevante sulla continuità dei servizi essenziali prestati (se sono operatori di servizi essenziali);
2. un impatto sostanziale sulla fornitura di un servizio digitale (nel caso di fornitori di servizi digitali).

La direttiva opera un'importante distinzione tra gli impatti rilevanti riferiti ai servizi essenziali e quelli sostanziali, riferiti, invece, ai servizi digitali. Vediamo qual è il significato di entrambi.
Un incidente è considerato rilevante sulla base dei seguenti criteri: il numero di utenti interessati dalla perturbazione del servizio essenziale; la durata dell'incidente e la diffusione geografica relativamente all'area interessata dall'incidente.
Per determinare, invece, se un incidente è sostanziale occorrerà tenere conto:

- del numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi;
- della durata dell'incidente;
- della diffusione geografica relativamente all'area interessata dall'incidente;
- della portata della perturbazione del funzionamento del servizio;
- della portata dell'impatto sulle attività economiche e sociali[43].

Un'ultima iniziativa che merita di essere trattata ha visto la luce il 5 luglio 2016, momento in cui la Commissione ha adottato una comunicazione che stabilisce varie misure per affrontare la frammentazione del mercato della sicurezza informatica dell'UE, atte a rafforzare la resilienza dell'Europa in materia di sicurezza informatica e a favorire la promozione del settore della *cyber* sicurezza.
Tra le azioni programmate, sarà istituita una rete di gruppi di intervento per la sicurezza informatica in tutta l'Unione europea, con l'obiettivo di

[42] *Ibidem.*
[43] Direttiva 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*, n. 1148.

garantire una reazione rapida alle minacce e agli incidenti digitali. Sarà, inoltre, istituito il c.d. 'gruppo di cooperazione' tra gli Stati membri per sostenere e facilitare la cooperazione strategica e lo scambio di informazioni e per aumentare la fiducia, in particolare in diversi settori dell'economia, comprese la formazione e l'istruzione in materia di sicurezza informatica[44].

[44] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 5 luglio 2016, n. 410, *Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cyber sicurezza*.

1.4 La normativa vigente in ambito *cyber* in Italia

Le prime politiche italiane in ambito *cyber* sono state sviluppate già a partire dagli anni Novanta ma anche esse si concentravano, per lo più, sul contrasto ai crimini informatici. Ne sono un esempio la legge n. 547 del 23 dicembre 1993, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, e la legge n. 269 del 3 agosto 1998, *Norme contro lo sfruttamento della prostituzione, della pedopornografia, del turismo sessuale in danno di minori*, la quale ha attribuito all'organo del Ministero dell'Interno deputato alla sicurezza e alla regolarità dei servizi di telecomunicazione, ossia la Polizia postale e delle comunicazioni, il dovere di intraprendere tutte le attività necessarie a contrastare il cybercrime (art. 14).
Nel corso degli anni 2000, invece, l'Italia ha iniziato a concentrare l'attenzione sulla necessità di garantire la protezione delle informazioni in formato digitale, con particolare riferimento ai *database* delle Pubbliche Amministrazioni. Questo perché, come la stessa la direttiva del 16 gennaio 2002 sulla *Sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni* emanata dal Ministro per le Innovazioni e tecnologie di intesa con il Ministro delle Comunicazioni ha stabilito, "le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese"[45] e devono, pertanto, essere protette in maniera efficace. A tal fine, la direttiva invita le Pubbliche Amministrazioni ad effettuare delle valutazioni dei loro sistemi informatici per verificarne il livello di sicurezza e, nel caso, provvedere a mettere in atto le misure necessarie per assicurare una base minima di sicurezza[46].
La direttiva del 2002 è soltanto il primo documento in Italia che si rivolge alle Pubbliche Amministrazioni, prendendo in considerazione l'importanza dei dati e delle informazioni da queste detenute e che pone, quindi, le basi per i successivi *steps* in materia di *cyber security*.
Già nel 2003, infatti, il Ministero delle Comunicazioni, di concerto con il Ministero della Giustizia e il Ministero dell'Interno, emana un decreto[47] mediante il quale viene istituito l'Osservatorio permanente per la sicurezza delle reti e la protezione delle comunicazioni. Lo scopo dell'Osservatorio è quello di "promuovere interventi normativi, regolamentari ed amministrativi, anche in relazione alle esigenze investigative di competenza dei dicasteri dell'interno e della giustizia"[48].
Sempre nel 2003 sono stati approvati altri due documenti rilevanti che riguardano rispettivamente la protezione dei dati personali e la tutela delle comunicazioni elettroniche.

[45] Direttiva del Presidente del Consiglio dei ministri, Dipartimento per l'Innovazione e le Tecnologie del 16 gennaio 2002, n. 69, sulla *Sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni*.
[46] *Ibidem*.
[47] Decreto interministeriale del 14 gennaio 2003.
[48] *Ibidem.*

Il primo di questi è il decreto n. 196 del 30 giugno 2003, *Codice in materia di protezione dei dati personali*, che disciplina il trattamento dei dati personali per chiunque agisca nel territorio dello Stato italiano o in altro luogo comunque soggetto alla sua sovranità e chiunque utilizzi, per il trattamento di tali dati, strumenti situati all'interno dello stesso.
Il secondo è il decreto legislativo n. 259 del 1° agosto 2003, *Codice delle comunicazioni elettroniche*, il quale stabilisce la normativa relativa alle comunicazioni che avvengono mediante l'utilizzo di mezzi e/o apparecchi elettronici, definendone principi, obiettivi e obblighi incombenti su gestori e settore pubblico. Il decreto garantisce inoltre, all'art. 3, il rispetto di alcuni diritti inderogabili quali la libertà delle persone nell'utilizzo dei mezzi di comunicazione elettronica, il diritto di iniziativa economica e di esercizio in regime di concorrenza e la libera fornitura di reti e servizi.
Infine, lo stesso articolo, al terzo comma, stabilisce che eventuali deroghe al Codice debbano derivare esclusivamente da esigenze di difesa e sicurezza dello Stato, di protezione della salute pubblica, di tutela dell'ambiente, della riservatezza dei dati personali, e debbano essere stabilite per mezzo di specifiche disposizioni di legge o di disposizioni regolamentari di attuazione.
Il Codice individua anche un'Autorità nazionale di regolamentazione (ANR) la quale, in collaborazione con il Ministero dello Sviluppo economico, ha il compito di adottare tutte le misure previste dallo stesso Codice per il conseguimento degli obiettivi di cui sopra abbiamo parlato e la promozione dello sviluppo del mercato e degli interessi dei cittadini.
L'istituzione di tale autorità deriva direttamente dall'attuazione della direttiva europea 2002/21/CE, che aveva istituito un Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC, *Body of European Regulators for Electronic Communications*) e invitato gli Stati membri a predisporre le relative autorità nazionali di regolamentazione.
Un ulteriore aspetto rilevante del Codice riguarda l'articolo 16-bis che individua, presso il sopracitato Ministero, un CERT nazionale. Come specificato dall'articolo 16-bis del Codice, il CERT svolge "compiti di assistenza tecnica in caso di segnalazioni da parte di utenti e di diffusione di informazioni anche riguardanti le contromisure adeguate per i tipi più comuni di incidente". Dopo un lungo periodo di studio e sperimentazione, il CERT nazionale ha avviato le sue attività a partire dal 5 giugno 2014 presso l'Istituto Superiore delle comunicazioni e delle tecnologie.
Ancora, nello stesso anno è il Ministero per l'Innovazione e le tecnologie a compiere un'ulteriore passo verso la definizione di un quadro legislativo più ampio in materia di *cyber security* attraverso la creazione di un Gruppo di lavoro sulla protezione delle infrastrutture critiche informatizzate composto sia da membri provenienti dal settore pubblico (principalmente si tratta dei rappresentanti dei Ministeri dell'Interno, delle Infrastrutture e delle Comunicazioni) sia dal settore privato (parliamo dei maggiori *provider* privati, tra cui Telecom Italia e Wind)[49].

[49] CENCETTI (2014: 67).

Tale gruppo pubblica nel 2004 un rapporto, che è stato un punto di riferimento per lo sviluppo della *cyber security* in Italia, dal seguente titolo: '*Protezione delle infrastrutture critiche informatizzate. La realtà italiana*'. In esso, si mette in luce la necessità di proteggere le infrastrutture critiche del Paese poiché, come abbiamo avuto modo di vedere, la loro tutela è fondamentale per la sicurezza dello stesso e il benessere dei cittadini. Il rapporto auspica, inoltre, la creazione di un Comitato e di un CERT-PA in grado di agire come sistema di allarme per la Pubblica Amministrazione, attivo 24 ore su 24, tutti i giorni della settimana; per quanto riguarda quest'ultimo, esso è divenuto operativo soltanto nel 2014.
Un altro passo fondamentale si compie nel 2005 con il decreto legislativo n. 82 del 7 marzo, *Codice dell'amministrazione digitale*, mediante il quale cittadini e imprese hanno ottenuto il diritto di comunicare in via telematica con le Pubbliche Amministrazioni e con i gestori di pubblici servizi. In questo modo, essi possono accedere ai documenti amministrativi attraverso l'utilizzo della rete.
Ad ogni modo, rilevante ai fini della nostra analisi è soprattutto l'articolo 51 del decreto, dedicato alla sicurezza dei dati, il quale stabilisce che:

> le norme di sicurezza definite nelle regole tecniche […] garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati
>
> [e che]
>
> i documenti informatici delle Pubbliche Amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

Il Codice dell'amministrazione digitale, dunque, non soltanto ha permesso un'accelerazione del processo di digitalizzazione della Pubblica Amministrazione ma ha anche sottolineato l'importanza della sicurezza e della protezione dei dati e delle informazioni personali.
Sempre nel 2005, vi è l'approvazione della legge n. 155 del 31 luglio 'recante misure urgenti per il contrasto del terrorismo internazionale', la quale si occupa anche della sicurezza telematica. All'articolo 7-bis, infatti, si afferma che l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (vale a dire il CNAIPIC, Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche, istituito nel 2008 e posto sotto la direzione della Polizia postale) è responsabile dell'attuazione del c.d. *law enforcement* in caso di attacchi informatici a infrastrutture critiche. Il CNAIPIC, inoltre, opera in stretta collaborazione sia con il CERT nazionale sia con il CERT PA, al fine di migliorare la capacità di risposta ad eventuali attacchi informatici attraverso un più coordinato scambio di informazioni.
Al fine di assicurare una maggiore protezione la legge istituisce, inoltre, un centro nazionale esclusivamente dedicato alla *Critical Information*

Infrastructure Protection.Il tema relativo alla protezione delle infrastrutture critiche ritorna ad essere oggetto di discussione nel 2008, quando il Ministero dell'Interno approva un documento che stabilisce le procedure nazionali per la classificazione delle infrastrutture critiche dell'Italia e propone una definizione di infrastrutture critiche nazionali, ossia tutti i sistemi e i servizi informatici di supporto a:

- ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute;
- Banca d'Italia ed autorità indipendenti;
- società partecipate dallo Stato, dalle Regioni e dai Comuni con più di 500.000 abitanti, nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque;
- ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività sia riconosciuta di interesse nazionale[50].

Nello stesso anno viene anche approvata la legge n. 48 del 18 marzo 2008, *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica*, tramite la quale si autorizza il Presidente della Repubblica a ratificare la Convenzione internazionale di Budapest sul *cyber crime*, firmata dall'Italia nel 2001. La partecipazione del Paese alla Convenzione si inserisce all'interno di un quadro più grande che vede diversi Paesi impegnati nell'affrontare la minaccia cibernetica non soltanto a livello nazionale ma anche a livello transnazionale.
Negli anni successivi, il processo di incremento del livello generale di digitalizzazione del Paese continua, in linea con quanto accade anche in altri Paesi, soprattutto europei.
Si arriva al 2010, anno in cui le procedure nazionali per la prevenzione, la gestione e la risposta delle/alle crisi vengono adeguate a quelle già elaborate nell'ambito della NATO e dell'Unione europea attraverso l'approvazione da parte della Presidenza del Consiglio dei ministri del DPCM del 5 maggio 2010, *Organizzazione nazionale per la gestione delle crisi.*
L'obiettivo è quello di aggiornare il Manuale nazionale per la gestione di crisi, pubblicato nel 1994 e rimasto valido per sedici anni e lo si fa lasciando al CoPS (Comitato politico-strategico), già previsto da Manuale del 1994, il ruolo di indirizzo e di guida nelle situazioni di crisi nazionale e, allo stesso tempo, introducendo una novità riguardante la composizione di tale organo: ai rappresentanti di Ministero degli Affari Esteri, Ministero degli Interni e Ministero della Difesa si aggiungono quelli del Ministero dell'Economia e

[50] Decreto del Ministero dell'Interno del 9 gennaio 2008, *Individuazione delle infrastrutture critiche informatiche di interesse nazionale*.

Finanza. Tale scelta è stata una dimostrazione dell'importanza della dimensione economica della sicurezza nazionale.
L'articolo 5 del decreto predispone poi l'istituzione di un nuovo organo: il Nucleo interministeriale di situazione e pianificazione (NISP) che va ad assorbire tutte le competenze del Nucleo politico militare (NPM), previsto dal manuale del 1994, nello svolgimento delle attività di consulenza al CoPS in caso di crisi, nonché di controllo e valutazione in condizioni di normalità.
Il NISP inoltre, come già l'NPM, ha assunto carattere permanente e svolge attività di monitoraggio costante della situazione di sicurezza interna ed internazionale. Infine, promuove la programmazione e la pianificazione interministeriale, acquisisce informazioni e coordina lo svolgimento delle esercitazioni interministeriali, che consistono nella simulazione di crisi[51].
Il decreto del 2010 dunque, oltre ad aggiornare l'organizzazione delle procedure di gestione delle situazioni di crisi, introduce alcune novità. Tra queste, la più rilevante riguarda senza dubbio l'inserimento del NISP all'interno del panorama degli organi deputati alla sicurezza nazionale e, di fatto, negli anni questo ha assunto sempre di più un ruolo fondamentale per la *cyber security* in Italia.
A tal proposito, altrettanto importante è la 'Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico' del Comitato parlamentare per la sicurezza della Repubblica (COPASIR), trasmessa alle due Camere del Parlamento italiano il 15 luglio 2010 e la cui funzione consiste nel fornire alle Camere indagini approfondite sui temi di maggior rilevanza per la sicurezza nazionale e internazionale. All'interno di questo documento la minaccia cibernetica viene esplicata in quattro grandi categorie: la prima riguarda i *cyber crimes*; la seconda il fenomeno del *cyber terrorism*; la terza il *cyber espionage*; infine, l'ultima, la *cyber war*. Anche in questo documento, come accade nella Raccomandazione dell'Organizzazione per la Cooperazione e lo Sviluppo Economico del 6 maggio 2014 *sulla governance dei rischi maggiori,* si afferma che per affrontare tali minacce l'approccio migliore risulta essere di tipo sistemico, ovvero un approccio in grado di coinvolgere tutti i settori della società, tutti i livelli di governo e di garantire e stimolare, così, una *Public-Private Partnership*.
La relazione evidenzia, inoltre, l'importanza del ruolo del Sistema di informazione per la sicurezza della Repubblica soprattutto nelle attività di monitoraggio e controllo delle minacce che attentano alla sicurezza del Paese, fra le quali è presente quella cibernetica.
Di fatti, in seguito all'approvazione della legge n. 124 del 3 agosto 2007, *Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto,* che ha modificato la struttura dei servizi di *intelligence* italiani[52],

[51] CENCETTI (2014: 67).
[52] Ora i servizi di *intelligence* sono così strutturati: alla base abbiamo il Dipartimento delle informazioni per la sicurezza (DIS), l' Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI); al livello intermedio vi è l'Autorità delegata per la sicurezza della Repubblica che viene designata dal Presidente del Consiglio in

sono state create al loro interno tre strutture che si occupano di *cyber security*: l'Ufficio centrale per la segretezza del Dipartimento delle informazioni per la sicurezza (DIS); la Sezione contro ingerenza telematica dell'Agenzia informazioni e sicurezza interna (AISI); la Divisione INFOSEC dell'Agenzia informazioni e sicurezza esterna (AISE).
Il Sistema di informazione per la sicurezza della Repubblica, in più, invia ogni anno una relazione al Parlamento relativa alla situazione attuale nel Paese, finalizzata a delineare il quadro di minacce a cui esso dovrà far fronte. Per la prima volta, nel 2010, all'interno di questa relazione si inserisce tra le sfide future e gli scenari di rischio la c.d. *cyber threat*, minaccia cibernetica per l'appunto.
Anche il 2011 è un anno importante per lo sviluppo della normativa italiana in ambito *cyber*.
Si torna a parlare di infrastrutture critiche con il decreto legislativo emanato dal Presidente della Repubblica n. 61, *Attuazione della direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione*, relativo alle procedure per l'individuazione e la designazione delle infrastrutture critiche europee, soprattutto per quanto riguarda i settori dell'energia e dei trasporti, nonché alle modalità di valutazione della sicurezza di tali infrastrutture e le relative prescrizioni minime di protezione dalle minacce di varia natura.
Lo stesso anno il decreto del Presidente del Consiglio dei ministri del 12 ottobre 2011 istituisce presso la Presidenza del Consiglio un Gruppo di studio per la sicurezza dell'utilizzo dello spazio cibernetico.
Il 2012 è, invece, per l'Italia l'anno in cui con l'approvazione dei due decreti legislativi n. 69 e 70 del 28 maggio 2012 vengono recepiti nell'ordinamento interno le direttive europee 2009/136/CE e 2009/140/CE e il regolamento (CE) 2006-2004 sulla cooperazione tra le autorità nazionali responsabili di tutelare i consumatori e vengono modificati il decreto legislativo n. 196 del 30 giugno 2003, recante codice in materia di protezione dei dati personali e il decreto n. 259 del 1° agosto 2003, recante codice delle comunicazioni elettroniche. L'obiettivo è armonizzare le varie disposizioni nazionali nell'ambito informatico e telematico.
Sempre nel 2012, l'Italia istituisce l'Agenzia per l'Italia Digitale (AdID)[53], la cui funzione è quella di:

> [coordinare] le azioni in materia di innovazione per promuovere le Ict (*Information and communication technologies*) a supporto delle Pubbliche Amministrazioni, garantendo la realizzazione degli obiettivi dell'Agenda digitale italiana[54], in coerenza con l'Agenda digitale europea[55].

---

relazione a particolari attività; infine, al vertice abbiamo il Comitato interministeriale per la sicurezza della Repubblica (CISR) ed il Presidente del Consiglio dei ministri.
[53] Mediante il decreto legge n. 83 del 15 giugno 2012, convertito in legge n. 134 del 7 agosto 2012.
[54] Stabilita con decreto del Ministero dello Sviluppo economico in data 1° marzo 2012.

Nel 2012 viene anche modificata la legge del 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto, con la legge n. 133 del 7 agosto 2012 che attribuisce al DIS un ruolo di coordinamento anche in relazione alle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali, sulle quali vigila il COPASIR. In tal modo, si è assegnato al DIS un ruolo certamente fondamentale in questo settore.
L'anno successivo è un anno di svolta: viene approvato dal Presidente del Consiglio dei ministri il decreto del 22 gennaio 2013 *recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale* mediante il quale, per la prima volta, viene definita "l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali"[56]. In esso, vengono sostanzialmente individuati gli organi e gli enti nazionali incaricati di gestire eventuali situazioni di emergenza che possono prodursi in seguito ad eventi malevoli verificatisi nel *cyber* spazio. Nello specifico, al Presidente del Consiglio viene assegnato il compito di elaborare un Quadro strategico nazionale per la sicurezza dello spazio cibernetico e un Piano nazionale per la protezione cibernetica e la sicurezza informatica, su proposta e delibera del Comitato interministeriale per la sicurezza della Repubblica (CISR). Inoltre egli, sentito il CISR, impartisce le direttive a DIS, AISE e AISI.
Il Comitato interministeriale per la sicurezza della Repubblica svolge, a sua volta, le seguenti attività:

1. alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico;
2. approvazione delle linee di indirizzo al fine di favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, la condivisione delle informazioni e, infine, l'adozione di *best practices* e di misure rivolte all'obiettivo della sicurezza cibernetica;
3. elaborazione degli indirizzi generali e degli obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali;
4. promozione dell'adozione di iniziative necessarie ad assicurare la piena partecipazione dell'Italia alle diverse forme di cooperazione internazionale (sia in ambito bilaterale sia multilaterale), finalizzate alla definizione e adozione di politiche e strategie comuni di prevenzione e risposta;

[55] Legge del 7 agosto 2012, n. 134, conversione in legge, con modificazioni, del decreto legge del 15 giugno 2012, n.83, recante *Misure urgenti per la crescita del Paese*.
[56] Decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*.

5. formulazione delle proposte di intervento normativo e organizzativo ritenute necessarie a potenziare le misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle crisi;
6. partecipazione, con funzioni di consulenza e di proposta, alle determinazioni del Presidente, in caso di crisi[57].

Presso la scuola di formazione istituita all'interno del Sistema di informazione per la sicurezza della Repubblica viene creato, poi, un Comitato scientifico di esperti di sicurezza cibernetica aventi la funzione di formulare ipotesi di intervento con la finalità di aumentare il livello di sicurezza nel *cyber space*.
Il decreto contiene anche una serie di definizioni utili a far chiarezza su alcuni concetti fondamentali quando si parla di *cyber security*, fra i quali il concetto di spazio cibernetico, di evento cibernetico e di minaccia cibernetica.
Sempre nel 2013, viene istituito presso l'Ufficio del Consigliere militare del Presidente del Consiglio il Nucleo per la sicurezza cibernetica, composto da un rappresentante per ciascuno dei seguenti enti:

- DIS;
- AISE;
- AISI;
- Ministero degli Affari esteri;
- Ministero dell'Interno;
- Ministero della Difesa;
- Ministero dello Sviluppo economico;
- Ministero dell'Economia e Finanza;
- Dipartimento della Protezione civile;
- Agenzia per l'Italia Digitale [58].

Esso svolge funzioni di raccordo tra le diverse componenti dell'architettura istituzionale coinvolte a vario titolo nell'ambito della sicurezza cibernetica. Più nello specifico, nel campo della prevenzione e della preparazione ad eventuali situazioni di crisi, il Nucleo promuove la programmazione e la pianificazione operativa della risposta a tali situazioni da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile; mantiene attiva, 24 ore su 24, 7 giorni su 7, l'Unità per l'allertamento e la risposta a situazioni di crisi cibernetica; valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della sicurezza cibernetica, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione

[57] CENCETTI (2014: 84 ss.).
[58] *Ibidem*.

delle crisi; acquisisce, sia dall'estero sia grazie al Ministero dello Sviluppo economico, agli organismi di informazione per la sicurezza, alle Forze di polizia e alle strutture del ministero della Difesa, le comunicazioni relative a casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significative ai fini del corretto funzionamento delle reti e dei servizi.
Esso rappresenta anche il punto di riferimento nazionale per i rapporti con l'Organizzazione delle Nazioni Unite, la NATO e l'Unione europea.
Inoltre, promuove e coordina, di concerto con il Ministero dello Sviluppo economico e con l'Agenzia per l'Italia Digitale per i profili di rispettiva competenza, lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica.
A tutto ciò, dobbiamo aggiungere la direttiva del Presidente del Consiglio del 1° agosto 2015, considerata strategica in quanto individua "le azioni prioritarie propedeutiche allo sviluppo di un sistema in grado di garantire, sempre di più, la protezione cibernetica e la sicurezza informatica".
Questa direttiva si pone in continuità con il percorso delineato dalla legge 133/2012 e il DPCM del 24 gennaio 2013, mediante i quali si è istituita quell'architettura istituzionale, di cui abbiamo parlato precedentemente, composta dai diversi attori che operano nel contesto *cyber*.
In più, al suo interno si delinea chiaramente qual è l'obiettivo primario per il Paese: il consolidamento di un sistema di reazione in grado di operare rapidamente e in maniera efficace qualora si verifichino incidenti o azioni ostili nei confronti delle infrastrutture informatiche nazionali.
Infine, essa specifica le misure da prendere per raggiungere questo obiettivo. Tra le più importanti possiamo citare la realizzazione di un coordinamento istituzionale che garantisca la condivisione e la circolarità delle informazioni, potenziando così l'operatività degli assetti trasversali previsti dal sistema di reazione: il Nucleo per la Sicurezza Cibernetica, il CERT Nazionale e il CERT-PA, l'ulteriore sviluppo di un partenariato pubblico-privato e, da ultimo, una sempre maggiore collaborazione con Università e Centri di ricerca finalizzati alla formazione di esperti nel settore.

Il 2017: le ultime novità in ambito cyber

Per quanto riguarda il 2017, il percorso verso più efficaci ed incisive politiche di *cyber security* è ancora in corso.
Definiamone le tappe più importanti.
Con il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*, l'Italia riorganizza l'architettura istituzionale nata nel 2013 rendendola più snella ed efficace mediante l'assegnazione di un ruolo ancor più decisivo al DIS.
Questo nuovo provvedimento rafforza anche il ruolo del CISR, riconduce il Nucleo sicurezza cibernetica all'interno del DIS con la funzione di

assicurare una risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale in raccordo con tutte le strutture dei Ministeri competenti in materia e prevede una forte interazione tra il Dipartimento della funzione pubblica, il Ministero dello sviluppo economico, il Ministero dell'interno, il Ministero dell'economia e finanza, il Ministero della difesa e l'Agenzia per l'Italia Digitale .
Infine, il decreto attribuisce al Direttore generale del DIS il compito di definire le linee di azione per incrementare il livello di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici sia privati, cercando anche di individuare ed eliminare eventuali vulnerabilità. Al fine di realizzare quanto previsto, viene presa in considerazione la possibilità di avvalersi di risorse di eccellenza provenienti dal mondo accademico e della ricerca nonché delle imprese di settore.
Risale invece a marzo l'uscita della Circolare AgID, n. 1/2017, recante le '*misure minime di sicurezza Ict per le Pubbliche Amministrazioni*', emesse dall'Agenzia per l'Italia Digitale nell'esercizio dei suoi poteri di dettare indirizzi, regole tecniche e linee guida in materia di sicurezza informatica, anche in ottemperanza alla direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri.

Concludiamo affermando che, come abbiamo potuto vedere, diverse sono le iniziative volte a disciplinare il *cyber* spazio sia a livello nazionale sia a livello regionale; tuttavia, ciò non basta. È necessario compiere ulteriori passi in avanti al fine di migliorare le proprie capacità di prevenzione e di risposta ad eventuali attacchi informatici, soprattutto se teniamo conto del fatto che ancora manca un'armonizzazione della disciplina in materia a livello internazionale: ciò mina l'efficacia delle diverse politiche nazionali di sicurezza informatica, laddove queste esistano, data la transnazionalità che caratterizza i *cyber attack*s.

CAPITOLO II

IL NUOVO FENOMENO DELLA *CYBER WAR* E LE IMPLICAZIONI DAL PUNTO DI VISTA DEL DIRITTO INTERNAZIONALE

L'avvento di Internet e della tecnologia informatica ha causato un mutamento epocale nelle dinamiche della società moderna sia civile sia militare[59]. Negli ultimi anni, in particolare, l'interesse sulle questioni legali riguardanti i problemi e le ostilità generate attraverso il *cyber* spazio è stato particolarmente elevato. La rete ha aperto un nuovo spazio conflittuale, un teatro artificiale di guerra supplementare ai teatri naturali di terra, d'aria, di mare e di spazio[60], che ha la capacità, inoltre, di essere interconnesso con tutti loro indipendentemente dalle frontiere.
A livello nazionale, alcuni Stati hanno già provveduto ad attuare una strategia di *cyber defence*.
A livello internazionale, ci si è mossi soprattutto per quanto riguarda la commissione di *cyber crimes* mentre occorre ancora capire se vi siano già norme valide in caso di *cyber war* (guerra cibernetica), che rappresenta oggi la nuova dimensione del conflitto internazionale, o se al contrario sia necessario elaborare un nuovo *framework* legale.
In questo capitolo analizzeremo, allora, il contenuto della Carta delle Nazioni Unite, focalizzandoci sulle regole esistenti che disciplinano l'uso della forza nella Comunità internazionale, e le norme internazionali relative alla disciplina dei conflitti armati alla luce dell'innovazione tecnologica che caratterizza l'epoca contemporanea e che, certamente, ha in parte modificato le tecniche di guerra.
Il fine ultimo consisterà nel dimostrare se sia possibile applicare le medesime regole, già esistenti, a questa nuova forma di *cyber* conflittualità.

[59] DINNISS (2012: 25-27).
[60] NILS (2011: 3).

2.1 Applicazione dello *jus ad bellum* e dello *jus in bello* alla luce del concetto di *cyber war*

Prima di procedere con l'analisi delle norme internazionali riguardanti l'uso della forza tra Stati (*jus ad bellum*) e la condotta dei conflitti armati (ossia il diritto internazionale umanitario o *jus in bello*[61]) definiamo il concetto di *cyber war*.
Con tale espressione indichiamo l'insieme delle condotte poste in essere nel *cyber* spazio per manipolare, sabotare, danneggiare o distruggere sistemi informatici e/o obiettivi civili e militari ad essi connessi, al fine specifico di causare effetti corrispondenti alla minaccia o all'uso della forza armata, prima e/o durante un conflitto che vede la partecipazione di uno o più soggetti di diritto internazionale[62].
Questo avviene mediante le cosiddette *cyber operations* (o *Computer network operations* – CNO), ossia attraverso l'impiego delle capacità cibernetiche con il proposito primario di raggiungere obiettivi all'interno o mediante l'uso del *cyber* spazio[63].
Secondo il Dipartimento di Difesa degli Stati Uniti le *cyber operations* possono essere distinte in tre categorie differenti:

a) *computer network exploitation* (CNE). Si tratta di operazioni di *intelligence* attuate con lo scopo di raccogliere dati da una rete o da un sistema informativo automatizzato;
b) *computer network defence* (CND). In tal caso, ci riferiamo a tutte quelle azioni intraprese per proteggere, monitorare, analizzare, rilevare e rispondere alle attività non autorizzate nei sistemi informativi del Ministero della difesa e nelle reti informatiche[64];
c) *computer network attack* (CNA). Esse comprendono tutte quelle operazioni finalizzate a disturbare, negare, degradare, distruggere le informazioni contenute all'interno di computer o reti di computer, o i computer e le reti stesse. Solo le operazioni che rientrano in quest'ultima categoria, se qualificate come minaccia o uso della forza (aspetto che esamineremo nelle pagine successive), potrebbero dar vita ad una *cyber war*.

[61] Si fa riferimento ai seguenti trattati internazionali: le Convenzioni dell'Aja del 1899 e del 1907 relative alla condotta delle ostilità e al diritto di neutralità; le quattro Convenzioni di Ginevra del 1949 relative ala protezione delle vittime dei conflitti armati internazionali e i due relativi Protocolli del 1977 (il primo relativo ai conflitti armati internazionali, il secondo ai conflitti armati non internazionali). In via generale, il diritto internazionale relativo ai conflitti armati si distingue in regole relative ai mezzi e ai metodi di guerra e regole relative alle categorie protette.
[62] GRECO (2014: 18).
[63] SCHMITT (2013: 257 ss.).
[64] US Department of Defense, The *National Military Strategy for Cyber space operations*, 2006, reperibile *on-line*.

È importante sottolineare che per *cyber war* non si intende una specifica categoria di guerra disciplinata da regole proprie, bensì l'impiego di particolari strumenti tecnico-informatici durante una guerra di stampo tradizionale, così come definita dal Primo e dal Secondo Protocollo Aggiuntivo alle Convenzioni di Ginevra relative al diritto internazionale umanitario[65]. Questo perché, come già detto, nonostante il *cyber* spazio rappresenti un mondo virtuale esso non è un mondo a sé stante ma è comunque legato al mondo fisico. Allo stesso modo, non dobbiamo pensare che una *cyber war* possa produrre effetti soltanto nel mondo virtuale poiché attraverso azioni di questo tipo si può attentare lo stesso alla vita di altre persone o, in ogni caso, generare gravi danni i cui effetti possono ripercuotersi sul loro benessere.
A sostegno di quest'interpretazione vi è la stessa definizione di guerra, considerata una contesa tra due o più Stati attraverso le loro forze armate, con il fine di sopraffarsi vicendevolmente ed imporre le condizioni del vincitore[66]. Da quest'affermazione deduciamo che la natura dei conflitti armati non dipende, dunque, dal modo in cui li si conduce o dagli strumenti utilizzati poiché ciò che conta sono gli effetti o i danni prodotti da una determinata azione; questi sono gli unici elementi che vanno considerati e che ci possono consentire di definire la *cyber war* una 'guerra' per l'appunto anche dal punto di vista giuridico.
Nonostante l'avvento delle nuove tecnologie, dunque, la guerra è guerra e la sua natura non è mutata. Se questa affermazione è valida occorre, d'altro canto, indagare su quanto le norme già esistenti nell'ordinamento internazionale in materia di conflitti armati siano valide anche in caso di *cyber war*.
Consideriamo, innanzitutto, le norme pattizie.
Al momento, non esiste alcun trattato internazionale che disciplina la *cyber war*. Eppure, la mancanza di regole pattizie *ad hoc* non può costituire una ragione valida per non applicare le regole vigenti in materia di conflitti armati anche ai conflitti cibernetici, che quindi devono rispettare il diritto internazionale e, in special modo, il diritto internazionale umanitario. Anche il Comitato Internazionale della Croce Rossa si è pronunciato a favore di questa interpretazione[67], affermando che

> non vi può essere alcun dubbio che il diritto internazionale umanitario si applichi ai nuovi armamenti e all'impiego in guerra dei nuovi sviluppi tecnologici, come riconosciuto, tra l'altro, dall'articolo 36 del I Protocollo addizionale"[68].

Di conseguenza, se è vero che non esistono norme internazionali che esplicitamente disciplinano le operazioni informatiche, sembra altrettanto

[65] *Ivi*, p. 12.
[66] HERSCH (1952: 270).
[67] GRECO (2014: 14).
[68] Primo Protocollo Addizionale alle Convenzioni di Ginevra del 12 agosto 1949.

vero che eventuali operazioni informatiche nell'ambito di un conflitto armato possano essere attuate ma nel rispetto delle norme vigenti in materia.
Consideriamo ora un altro aspetto, che potrebbe aiutarci nella nostra analisi: quando si parla di *jus in bello* e *jus ad bellum*, fondamentale è la presenza di un costante bilanciamento tra il principio di umanità, definito dalla c.d. Clausola Martens del 1899, e il principio di necessità militare, contenuto nella Dichiarazione di San Pietroburgo del 1868. Analizziamoli entrambi.
La Clausola Martens è contenuta nel preambolo della Seconda Convenzione dell'Aia concernente le leggi e gli usi della guerra terrestre del 1899 e ha come fine quello di tutelare coloro che non partecipano direttamente alle ostilità in caso di conflitti armati non-internazionali.
Essa è stata, anche, inserita nell'art. 1, comma 2, del Primo Protocollo Addizionale del 1977 alle suddette Convenzioni, che recita:

> […] In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.

e nel preambolo del Secondo Protocollo Addizionale. Oggi, la Clausola Martens rappresenta un principio di diritto internazionale consuetudinario che viene per l'appunto definito 'principio di umanità'.

Il secondo principio, invece, riguarda il modo di condurre la guerra ed impone una valutazione continuativa dei combattenti sulla necessità, liceità e proporzionalità dell'uso della forza armata, così da stabilire un equilibrio tra la necessità militare e le esigenze umanitarie[69].

Entrambi questi principi sembrano trovare applicazione nel contesto delle operazioni informatiche.
Per quanto riguarda la Clausola Martens, è la stessa Corte internazionale di giustizia ad affermare che essa ha dimostrato di essere un mezzo efficace per affrontare la rapida evoluzione della tecnologia militare[70].
Per quanto riguarda, invece, il principio della necessità militare una sua applicazione al contesto cibernetico è ipotizzabile laddove si consideri ciò che è scritto nella Dichiarazione di San Pietroburgo e cioè che i progressi della civiltà devono produrre l'effetto di attenuare, nei limiti del possibile, le calamità della guerra e che il solo scopo legittimo che gli Stati devono prefiggersi durante la guerra è l'indebolire le forze militari del nemico[71].
La natura della *cyber war*, che non utilizza armi e che colpisce solo indirettamente la popolazione civile, risponde in qualche modo al fine ultimo del documento. Infatti, i danni prodotti da un attacco informatico, seppur

[69] Dichiarazione di San Pietroburgo del 1868.
[70] Parere della Corte internazionale di giustizia dell'8 luglio 1996 *sulla liceità della minaccia o dell'uso delle armi nucleari*.
[71] Dichiarazione di San Pietroburgo del 1868.

ingenti, non sono mai stati fino ad ora paragonabili a quelli prodotti da un attacco armato di tipo convenzionale.
Non possiamo, però, ancora affermare che oggi esista una prassi consolidata da parte degli Stati, attori fondamentali nel contesto cibernetico e del diritto internazionale, relativa all'applicazione delle norme dei conflitti armati al *cyber space*.
Nel prossimo paragrafo, esaminiamo, invece, nel dettaglio il ruolo delle Nazioni Unite e il contenuto del loro statuto alla luce del concetto di *cyber war*.

2.2 Le Nazioni Unite e il mantenimento della pace e della sicurezza internazionali

L'Organizzazione delle Nazioni Unite (ONU) nasce ufficialmente il 24 ottobre 1945 con l'entrata in vigore del proprio trattato istitutivo (la c.d. Carta delle Nazioni Unite).
Si tratta di un'organizzazione internazionale a vocazione universale i cui obiettivi sono: mantenere la pace a la sicurezza internazionali, sviluppare relazioni amichevoli tra le nazioni sulla base del rispetto dell'eguaglianza dei diritti e dell'autodeterminazione dei popoli, promuovere la cooperazione internazionale in materia economica, sociale e culturale, nonché il rispetto dei diritti dell'uomo e delle liberà fondamentali[72].
In questo paragrafo concentreremo la nostra attenzione sul ruolo delle Nazioni Unite circa il mantenimento della pace e della sicurezza internazionali.
A riguardo, l'architettura disposta dalla Carta prevede un divieto generale di ricorso alla forza armata, contenuto all'art. 2, par. 4 che recita:

> all Members shall refrain in their International relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Il divieto dell'uso della forza è un divieto di carattere assoluto che proibisce l'uso della forza o la sua minaccia agli Stati nelle loro relazioni internazionali[73]. Tale divieto non è ristretto, dunque, ai soli Stati membri dell'Organizzazione delle Nazioni Unite poiché è ormai oggi diventato un principio cardine del diritto internazionale.
Tuttavia, esistono delle eccezioni ad esso.
Nello specifico, parliamo del sistema di sicurezza collettiva che fa capo al Consiglio di sicurezza delle Nazioni Unite (articoli 39-41 della Carta) e della legittima difesa individuale e collettiva (articolo 51).

---

[72] Carta delle Nazioni Unite, San Francisco, 24 ottobre 1945, art. 1: "The Purposes of the United Nations are: 1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace; 2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace; 3. To achieve international cooperation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and 4. To be a center for harmonizing the actions of nations in the attainment of these common ends" .
[73]RONZITTI (2013: 414 ss.).

La sicurezza collettiva

Il sistema di sicurezza collettiva fa riferimento al Capitolo VII della Carta delle Nazioni Unite e prevede un'azione del Consiglio di Sicurezza per mantenere, o ristabilire, la pace e la sicurezza internazionali. Affinché ciò si realizzi è necessario, innanzitutto, che il Consiglio di Sicurezza accerti l'esistenza di una minaccia alla pace o di una violazione della stessa o di un atto di aggressione, ai sensi dell'art. 39 che recita:

> the Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

Avvenuto quanto detto sopra, il Consiglio di sicurezza può raccomandare oppure decidere l'adozione di misure coercitive non comportanti l'uso della forza armata[74].
Nel primo caso, si dà luogo ad atti giuridicamente non vincolanti, pertanto gli Stati membri non avranno l'obbligo di eseguire le misure raccomandate; nel secondo caso, invece, si tratta di atti giuridicamente vincolanti che pongono degli obblighi a carico degli Stati membri, i quali dovranno darvi esecuzione.
Per l'approvazione di ciascuna delibera è richiesto il voto favorevole di nove dei quindici membri che compongono il Consiglio di sicurezza, fra i quali devono esservi i cinque membri permanenti (Stati Uniti, Russia, Cina, Regno Unito e Francia) che, diversamente dagli altri dieci membri eletti a rotazione dall'Assemblea generale delle Nazioni Unite ogni due anni, godono del c.d. diritto di veto.
Attraverso l'esercizio di tale diritto questi cinque Paesi possono bloccare l'azione del Consiglio di Sicurezza ed è per tale ragione che è necessario un loro voto favorevole. Esiste, tuttavia, un'eccezione poiché anche una loro eventuale astensione ormai, per prassi, non viene interpretata come un ostacolo all'approvazione di una delibera. Questo, in realtà, si pone in contrapposizione con quanto si afferma nell'art. 27 della Carta delle Nazioni Unite (cioè che è necessaria l'espressione di un voto favorevole da parte degli Stati membri, soprattutto se parliamo dei cinque membri permanenti). Ad ogni modo, come già detto, con il consenso di tutti gli Stati membri, è stato apportato un emendamento alla Carta per consentire il corretto funzionamento del Consiglio di sicurezza anche laddove uno dei membri permanenti decida di astenersi.
Al contrario, la non partecipazione alla seduta impedisce l'approvazione della delibera. Sebbene alcune decisioni del Consiglio di sicurezza siano

[74] L'art. 41 detta in proposito un elenco non tassativo: "The Security Council may decide what measures […] These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations".

state prese in passato proprio grazie all'assenza di uno dei cinque membri permanenti[75], non possiamo affermare che si sia consolidata una prassi in tal senso. Parte della dottrina ritiene, in ogni caso, necessario interpretare l'assenza in conformità con la volontà dello Stato. Perciò, se uno Stato si assenta con l'obiettivo di paralizzare l'attività del Consiglio allora il suo atteggiamento deve essere interpretato come un voto negativo; qualora, invece, la sua assenza esprima la volontà di dissociarsi dall'atto che deve essere approvato allora il suo atteggiamento può essere paragonato all'astensione e, pertanto, non si impedisce in alcun modo l'adozione dell'atto stesso.
Per quanto riguarda l'art. 42, di cui si parla sopra, questo era stato originariamente pensato per permettere al Consiglio di Sicurezza di intervenire ricorrendo direttamente alla forza armata attraverso l'offerta di truppe da parte degli Stati membri. Tuttavia, questo articolo non ha mai trovato applicazione; in luogo di quanto recita l'art. 42, si è invece consolidata una prassi, che in materia ha svolto un ruolo di 'supplenza' mediante un'autorizzazione agli Stati all'uso della forza da parte del Consiglio di Sicurezza.
L'origine di tale procedura è da collocarsi nella prima fase della Guerra Fredda; più specificamente, nel 1950: durante la Guerra di Corea, infatti, il Consiglio di Sicurezza riuscì ad approvare (a causa dell'assenza del rappresentante dell'Unione Sovietica) una delibera con cui raccomandò l'intervento a favore della Corea del Sud; successivamente, autorizzò l'uso della bandiera delle Nazioni Unite da parte degli Stati che erano intervenuti e che operavano sotto il comando unificato degli Stati Uniti. Tale pratica non è altro che una delega delle funzioni del Consiglio di Sicurezza agli Stati; pertanto, questi dovrebbero operare nei limiti di tale delega o dell'autorizzazione ricevuta e sotto lo stretto controllo del Consiglio stesso, sebbene ciò non sempre avvenga.
Da notare che il Consiglio di Sicurezza può autorizzare gli Stati ad utilizzare la forza ma non può obbligarli a farlo[76].

A seguito di altri eventi storici, si è diffusa anche la prassi relativa ad un'autorizzazione all'uso della forza *ex post* avente una funzione sanatoria da parte del Consiglio di Sicurezza di un atto che, di per sé, sarebbe in contrasto con l'art. 2, par. 4 della Carta delle Nazioni Unite.

[75] Ciò è accaduto negli anni Cinquanta, durante la Guerra Fredda. Nello specifico, lo Stato membro permanente assente era l'Unione Sovietica che, in quel momento, protestava mediante la sua non partecipazione alle sedute del Consiglio di sicurezza contro la mancata sostituzione della Repubblica Popolare Cinese (proclamata il 1° ottobre del 1949, in seguito alla vittoria dei comunisti guidati da Mao Tse Tung sui nazionalisti, rifugiatisi a Taiwan) alla Cina nazionalista in seno al Consiglio. La protesta dell'URSS durò sei mesi ma il Consiglio di sicurezza, nonostante l'abbandono delle sedute da parte del Paese, approvò ben due delibere. Secondo alcuni Stati, infatti, la non partecipazione alle sedute era equiparabile all'astensione. Tuttavia, il consenso da parte dei membri delle Nazioni Unite in tal senso non è stato tale da trasformare questo in una norma consuetudinaria come avvenuto per il non voto.
[76] RONZITTI (2013: 460).

Quale esempio, possiamo citare la risoluzione 1244-1999 del Consiglio di Sicurezza che ha regolarizzato a posteriori l'azione della Nato contro la Repubblica Federale di Iugoslavia[77]. Tuttavia, questa non risulta essere ancora una prassi consolidata e supportata dal consenso unanime della Comunità internazionale.
Da respingere senza alcun dubbio invece, secondo parte della dottrina[78], la tesi per cui il Consiglio di Sicurezza possa autorizzare implicitamente gli Stati ad usare la forza[79].

La legittima difesa individuale e collettiva

L'art. 51 della Carta delle Nazioni Unite afferma che

> nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations until the Security Council has taken the measures necessary to maintain international peace and security.

Questo articolo autorizza, dunque, tutti gli Stati che subiscono un attacco armato a reagire mediante l'uso della forza. Diversamente, gli Stati che subiscono un uso della forza diverso da un attacco armato dovranno ricorrere ad altre misure se desiderano rispondere in maniera lecita; essi potrebbero, ad esempio, adottare delle contromisure[80].
Occorre precisare che, nonostante la Carta preveda la liceità della legittima difesa solo dopo che un attacco armato sia stato sferrato, le moderne tecniche di armamento hanno prodotto una modifica di tale limitazione: lo stesso *Panel di Alto Livello*, incaricato dal Segretario Generale delle Nazioni Unite di studiare la riforma della Carta si è pronunciato, nel suo rapporto del 2004,

[77] *Ivi*, p. 463.
[78] RONZITTI (2013: 463 ss.).
[79] *Ibidem*.
[80] La contromisura, nel diritto internazionale, è la forma più importante di autotutela. E' prevista dall'art. 22 e dagli articoli dal 49 al 53 del Progetto di articoli sulla responsabilità dello Stato della Commissione di diritto internazionale, i quali stabiliscono che, in seguito alla violazione di una norma di diritto internazionale da parte di un Stato, lo Stato leso è autorizzato ad adottare un comportamento, che in sé sarebbe illecito, ma che diviene lecito in quanto costituisce una reazione ad un illecito altrui. In altri termini, lo Stato leso può, per reagire contro lo Stato autore dell'illecito, violare a sua volta, ovviamente nei confronti di quest'ultimo, gli obblighi che derivano da norme consuetudinarie, da norme convenzionali e da norme contenuti in decisioni di organi internazionali, per reintegrare l'ordine giuridico violato. Essa dovrebbe consistere in una azione che, nella misura del possibile, abbia effetti temporanei e reversibili. La contromisura incontra vari limiti, tra cui la proporzionalità della violazione subita e la violazione commessa per rappresaglia. Un altro limite è quello dell'impossibilità di ricorrere a violazioni del diritto internazionale cogente, anche nel caso in cui si tratta di reagire a violazioni dello stesso tipo. Altri limiti sono il rispetto dei principi umanitari e il limite del previo esaurimento dei mezzi di soluzione delle controversie. Infine non possono essere prese contromisure e, se già prese, devono essere sospese senza indebito ritardo, se: a) l'atto internazionalmente illecito è cessato; e se b) la controversia pende innanzi ad una corte o ad un tribunale che abbia il potete di adottare decisioni vincolanti per le parti.

a favore della legittima difesa sia dopo che abbia avuto luogo un attacco armato sia nell'imminenza dello stesso[81]. Ad ogni modo, la nozione di 'imminenza di un attacco armato' deve essere intesa in senso restrittivo, per evitare abusi[82]. Inoltre, affinché il diritto di legittima difesa possa essere esercitato, occorre che si sia verificata una violazione dell'art. 2, par. 4 particolarmente qualificata: occorre, dunque, che si sia verificato un attacco armato[83]. Questo può essere compiuto non soltanto mediante le forze armate di uno Stato, ma anche mediante gruppi armati non immediatamente inquadrabili nell'organizzazione politico-militare di uno Stato bensì agenti sotto le sue direttive, di modo che gli atti compiuti siano a questo imputabili[84].

L'art. 51 non precisa, invece, se l'attacco armato debba provenire soltanto da uno Stato o anche da un'entità non statale. L'*Institut de droit international*[85], nella sessione di Santiago del 2007, ha adottato una risoluzione secondo la quale si può usare la forza in risposta ad un attacco armato proveniente da un'entità non statale contro lo Stato territoriale qualora l'entità in questione abbia agito su istruzione, direzione o controllo di tale Stato; nel caso in cui l'attacco provenga da un'area non sottoposta alla giurisdizione di alcuno Stato si potrà, invece, reagire contro l'entità non statale stessa in quest'area.

Da ultimo, l'art. 51 prevede che la reazione in legittima difesa sia esercitata nei limiti posti dai due criteri della necessità e della proporzionalità[86], non espressamente menzionati nella Carta ma riconosciuti quali norme consuetudinarie[87] che, pertanto, hanno efficacia *erga omnes*, ossia nei confronti di tutti i soggetti di diritto internazionale.

Per quanto riguarda il criterio della necessità, la prassi e la dottrina fanno spesso riferimento al caso *Caroline* (1837): qui si afferma che la forza può essere esercitata qualora sussista una "necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation". In altre parole, si richiede che l'uso della forza sia l'unica risposta possibile per respingere efficacemente un attacco in corso.

Per quanto riguarda il criterio della proporzionalità, rileva l'interpretazione alquanto restrittiva offerta dalla Corte internazionale di giustizia nel caso

---

[81] *Report* del 1 dicembre 2004, *on Threats, Challenges and Changes, A more secure world : our shared responsibility*.

[82] RONZITTI (2013: 422).

[83] *Ibidem.*

[84] Si tratta della c.d. aggressione indiretta, presa in considerazione dall'art. 3 (g) della risoluzione sulla definizione di aggressione dell'Assemblea Generale delle Nazioni Unite (ris. 3314-XXIX), disposizione che la Corte internazionale di giustizia, nell'affare *Nicaragua c. Stati Uniti*, ha detto appartenere al diritto internazionale generale.

[85] Fondato l'8 settembre del 1873 a l'Hotel de ville de Gand, in Belgio, da un gruppo di 11 internazionalisti con l'obiettivo di creare un'istituzione indipendente dall'influenza dei governi che contribuisca allo sviluppo del diritto internazionale e che agisca per la sua applicazione.

[86] RONZITTI (2013: 425).

[87] Sentenza della Corte internazionale di giustizia del 27 giugno 1986 nel caso delle *Attività militari e paramilitari degli Stati Uniti in Nicaragua e contro il Nicaragua (Nicaragua c. Stati Uniti)*.

delle *piattaforme petrolifere*[88]: mediante il rispetto di tale criterio si mira ad una limitazione della quantità, della modalità, della durata, dell'intensità, dello scopo e dei mezzi impiegati in risposta ad un attacco armato.
La legittima difesa ha, inoltre, un termine finale che coincide con l'intervento del Consiglio di Sicurezza, il quale è chiamato a prendere le misure necessarie per il mantenimento della pace e della sicurezza internazionali secondo quanto stabilito nel Capitolo VII della Carta delle Nazioni Unite. In ogni caso, lo Stato che agisce in legittima difesa ha, comunque, l'obbligo di informare il Consiglio di Sicurezza che, in tal modo, può accertare se l'azione intrapresa da questi sia lecita e non nasconda al contrario un atto di pura aggressione.

Il diritto all'autotutela è un diritto sia individuale, come abbiamo visto sino ad ora, sia collettivo.
Questa seconda ipotesi fa riferimento alla possibilità per un Stato terzo, non oggetto di alcun attacco armato, di intervenire a favore dello Stato attaccato.
Nello specifico, l'art. 51 prevede, innanzitutto, che lo Stato oggetto di attacco debba essere uno Stato membro delle Nazioni Unite; da una prima lettura sembrerebbe, allora, da escludersi la titolarità del diritto di legittima difesa collettiva nei confronti di quegli Stati non ancora membri delle Nazioni Unite. In passato sono sorte, in proposito, delle perplessità da parte della Comunità internazionale.
Tale questione è stata sollevata, ad esempio, in occasione dell'intervento degli Stati Uniti a favore del Vietnam del Sud durante gli anni della Guerra Fredda, non essendo questo ancora un membro delle Nazioni Unite, se non che per alcuni si era già avuta una modificazione integrativa dell'art. 51 nel senso di attribuire il diritto di difesa collettiva anche ai non membri.
A fugare ogni dubbio l'intervento della Corte internazionale di giustizia che, nel caso *Nicaragua c. Stati Uniti*, ha espressamente sancito l'appartenenza al diritto internazionale consuetudinario del diritto di legittima difesa collettiva[89], fruibile da tutti gli Stati della Comunità internazionale e non soltanto dagli Stati membri dell'Organizzazione delle Nazioni Unite.
Il diritto di legittima difesa collettiva, per essere esercitato, richiede la verifica delle medesime condizioni della legittima difesa individuale.
Di nuovo, ricordiamo che si ammette la liceità della legittima difesa (collettiva) sia dopo che l'attacco armato sia stato sferrato sia nell'imminenza di questo. A riguardo, occorre, tuttavia, aggiungere un'ulteriore limitazione per lo Stato terzo che intende intervenire: l'imminenza dell'attacco deve essere di una gravità tale che l'intervento in soccorso risulti assolutamente necessario, non potendo lo Stato oggetto della

[88] Sentenza della Corte internazionale di giustizia del 6 novembre 2003 relativa all'affare delle piattaforme petrolifere.
[89] Sentenza della Corte internazionale di giustizia del 27 giugno 1986 nel caso delle *Attività militari e paramilitari degli Stati Uniti in Nicaragua e contro il Nicaragua (Nicaragua c. Stati Uniti)*.

minaccia far fronte al futuro attacco con i propri mezzi[90]. Uno Stato non può, perciò, intervenire a favore di un altro senza che la vittima abbia verificato di essere oggetto di un attacco armato ed abbia richiesto l'intervento a suo favore. Ciò non toglie, tuttavia, che lo Stato interveniente debba a sua volta verificare che sussistano le condizioni per la legittima difesa; in caso contrario, qualora ricorresse all'uso della forza armata, rischierebbe di commettere un illecito internazionale, nonostante sia presente la richiesta di intervento da parte dello Stato che pretende di essere vittima di un attacco armato, imminente o in atto.

[90] RONZITTI (2013: 441).

2.3 *Computer network* attacks: cosa dice la Carta delle Nazioni Unite

In ragione di quanto sinora esaminato, in questo paragrafo ci si porrà l'obiettivo di verificare quanto la Carta delle Nazioni Unite sia applicabile anche ai *computer network attacks* e quanto, invece, il suo testo sia meritevole di una revisione mirata al fine di attagliarlo anche al contesto cibernetico.
Secondo la gran parte degli studiosi le previsioni contenute nella Carta delle Nazioni Unite possono essere applicate anche ai *computer network attacks*, se qualificabili quali minaccia o uso della forza.
Vi è, ormai, un largo consenso a livello internazionale per cui, nonostante la mancata menzione di questo tipo di attacchi nella Carta (per ovvi motivi storici), essi possano essere inseriti nella più generale categoria di attacco armato esplicitata nel documento[91].
Quest'asserzione si basa su quanto affermato dalla stessa Corte internazionale di giustizia nel parere del 1996 sulle armi nucleari, vale a dire che

> [le disposizioni della Carta si applicano] to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon […][92].

Pertanto, possiamo ritenere che il contenuto della Carta delle Nazioni Unite sia effettivamente applicabile a qualsiasi nuovo tipo di arma introdotta nel mondo contemporaneo, a prescindere dal fatto che questa sia o meno contemplata nel testo originale della stessa.
Se, come accennato, a riguardo esiste un certo *consensus*, risulta più difficile raggiungere tale accordo circa le circostanze in base alle quali tali disposizioni siano applicabili ai *computer network attacks* e, soprattutto, quali articoli possano trovare applicazione.
Segue, quindi, una rilettura degli articoli sopra esaminati (articoli 2, 39 e 51) al fine di verificare la loro applicabilità in ambito *cyber*.

Articolo 2, par. 4 : il divieto dell'uso della forza

Riprendendo quanto affermato nelle pagine precedenti, soffermiamoci a riflettere sul significato di quest'articolo.
In esso, si menzionano i concetti di uso e minaccia della forza.
Si tratta, tuttavia, di termini che racchiudono un significato complesso, spesso oggetto di discussione fra gli studiosi; ed è proprio l'incapacità di determinare con esattezza cosa si intende per uso o minaccia della forza a rendere più difficile la qualificazione di un attacco informatico come tale.

[91] HANDLER (2012: 209 ss.).
[92] Parere della Corte internazionale di giustizia dell'8 luglio 1996 *sulla liceità della minaccia o dell'uso delle armi nucleari*.

Una prima riflessione che dobbiamo fare riguarda il concetto di 'minaccia' e le sue implicazioni nell'uso della forza. Esclusi alcuni casi evidenti, come la presenza di un *ultimatum*[93], non è semplice identificare cosa possa costituire una minaccia. Anche la Corte internazionale di giustizia si è pronunciata in tal senso, escludendo peraltro che ricorra la minaccia di uso della forza nel caso in cui uno Stato metta a punto un notevole livello di armamenti: questo perché nel diritto internazionale consuetudinario non esistono delle regole che impongono agli Stati sovrani dei limiti di armamento.
Lo stesso vale nel caso in cui uno Stato, avente relazioni piuttosto tese con un altro, iniziasse aggressivamente a sviluppare la propria capacità di condurre operazioni informatiche potenzialmente dannose: la semplice acquisizione di tale capacità non costituirebbe una minaccia; qualora, invece, questo dichiarasse che questa sarà impiegata per fini bellici e contro lo Stato considerato ostile allora esso violerebbe l'art. 2, par. 4 della Carta delle Nazioni Unite ponendo in essere una minaccia all'uso della forza.
Secondariamente, riflettiamo sul significato del termine 'forza': parliamo soltanto di forza armata? In quali termini?
Secondo un'interpretazione sistematica della Carta si tratterebbe di forza armata, come confermato anche dagli stessi lavori preparatori allo statuto delle Nazioni Unite.
All'interno della stessa Carta possiamo notare come il termine forza talvolta sia esplicitamente accompagnato dalla precisazione che si tratta di forza armata (questo accade, ad esempio, nel Preambolo[94]); altre volte, laddove tale qualificazione non compaia, il contesto, comunque, induce chiaramente ad escludere il riferimento alla coercizione economica (a titolo d'esempio, è sufficiente leggere l'art. 44[95]). Nonostante una certa ambiguità letterale sia rimasta, comunque il pensiero prevalentemente accettato è quello che interpreta in senso univoco il termine 'forza' in riferimento alla forza armata o di tipo militare; nondimeno, alcuni Stati in passato hanno tentato di spingere in un altro senso l'interpretazione dell'art. 2[96].
Se questo è vero, d'altra parte occorre specificare che, invece, l'espressione 'forza armata' deve essere interpretata in maniera ampia, in modo da comprendere tanto il suo utilizzo diretto quanto quello in via indiretta. Consideriamo, a tal proposito, il caso *Nicaragua c. Stati Uniti*: qui, la Corte

[93] Ad es., il 13 ottobre 1998, la NATO lanciò un *ultimatum* alla Repubblica Federale di Iugoslavia affermando che avrebbe usato la forza qualora questa non avesse posto fine ai maltrattamenti della popolazione albanese in Kosovo e non avesse dato esecuzione alla ris. 1199-1998 del Consiglio di Sicurezza delle Nazioni Unite. L'*ultimatum* fu seguito dal c.d. ordine di attivazione e le forze aeree NATO avrebbero entro 96 ore iniziato i bombardamenti.
[94] "[…] to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used […]", Carta delle Nazioni Unite, San Francisco, 1945.
[95] "When the Security Council has decided to use force it shall, before calling upon a Member not represented on it to provide armed forces in fulfilment of the obligations assumed under Article 43, invite that Member, if the Member so desires, to participate in the decisions of the Security Council concerning the employment of contingents of that Member's armed forces", Carta delle Nazioni Unite, San Francisco, 1945.
[96]RONZITTI (2013: 414).

internazionale di giustizia ha affermato che addirittura le azioni poste in violazione del principio di non ingerenza, se prevedono l'uso diretto o indiretto della forza armata, possono costituire anche una violazione dell'art. 2, par. 4.
Con l'obiettivo di esaminare le sfaccettature del principio di non ingerenza e l'ipotesi di violazione del divieto all'uso della forza se ne riportano di seguito alcune possibili interpretazioni.
L'ingerenza non è altro che un'interferenza esercitata da uno Stato negli affari interni ed esterni di un altro Stato con lo scopo di condizionare l'esercizio della sovranità di quest'ultimo. Essa si caratterizza per la presenza di coercizione e imposizione della volontà.
Laddove, allora, le azioni di uno Stato non implicassero l'uso della forza armata ma consistessero in coercizioni di natura politica ed economica finalizzate a condizionare l'esercizio della sovranità, può comunque palesarsi l'ipotesi di una violazione dell'art. 2, par. 4 (sempre che sussistano certe condizioni).
Nel caso specifico analizzato dalla Corte è stato stabilito che, ad esempio, la mera fornitura di fondi ai ribelli costituisce semplicemente un atto di ingerenza negli affari interni (del Nicaragua in questo caso), ma non una violazione della proibizione dell'uso della forza. Al contrario, la fornitura di armi si sarebbe posta in violazione dell'art. 2, par. 4, in quanto finalizzata a influenzare e condizionare l'andamento degli eventi all'interno di un altro Stato. Allo stesso modo allora, il mero finanziamento di un gruppo di attivisti che conducono operazioni cibernetiche come parte di un'insurrezione non costituirebbe un uso della forza; al contrario, rifornire un gruppo organizzato con *malware* o con l'addestramento necessario finalizzato ad effettuare attacchi informatici si qualificherebbe come uso della forza.

Al fine di facilitare, allora, l'applicazione delle norme previste dalla Carta delle Nazioni Unite, diversi studiosi hanno elaborato teorie o modelli che potessero facilitare l'inquadramento degli attacchi informatici all'interno del *framework* legislativo offerto dalla Carta.
Uno di questi, l'esperto di diritto internazionale Michael Schmitt, ha proposto un test per determinare se e quando l'azione di uno Stato costituisca uso della forza armata, ponendosi in contrasto con l'art. 2, par. 4 della Carta delle Nazioni Unite e quando costituisca, invece, una forma di coercizione politica o economica.
Schmitt prende in considerazione sette fattori chiave da analizzare per giungere ad una conclusione[97].
Vediamoli nel dettaglio e tentiamo di applicarli ai *cyber attacks*.

1. la *severità (o gravità del danno).* Secondo Schmitt, essa prevede che solo gravi danni a persone o proprietà costituiscano uso della forza,

[97] WEISSBRODT (2017: 359).

mentre danni di minor impatto non ne rilevino la circostanza; perciò tutte quelle *computer network operations* che hanno un impatto critico sugli interessi nazionali potrebbero tendenzialmente essere considerate come un uso della forza armata. Inoltre, lo scopo, la durata e l'intensità di tali operazioni sono tutti fattori da analizzare al fine di determinare la severità di un attacco informatico e consentirne un inquadramento entro il concetto di attacco armato o meno;

2. l'*immediatezza*, vale a dire quanto velocemente si manifestano gli effetti di un attacco. Più breve è l'arco temporale entro il quale si verificano gli effetti di un attacco, tanto più alta sarà la probabilità che questo sia qualificabile come uso della forza; per quanto riguarda le *cyber network operations* l'immediatezza è, forse, una delle più ricorrenti peculiarità data la rapidità con la quale si propagano gli effetti di un *cyber attack* se paragonati agli effetti generati, invece, da un attacco armato convenzionale;
3. il *nesso di causalità*, cioè quando l'azione che si compie è l'unica causa degli effetti prodotti. Non si potrà, quindi, parlare di uso della forza quando il legame tra la causa e gli effetti si attenua. Comparando il nesso di causalità tra attacco armato convenzionale e *cyber attack* quest'ultimo risulterà, nella maggioranza dei casi, più difficilmente correlabile in maniera univoca agli effetti prodotti;
4. l'*invasività*, ossia il grado con il quale un'azione penetra e produce effetti all'interno dei confini di un altro Stato. Essa aumenta all'aumentare delle difese di un sistema incrementando, a sua volta, la probabilità di essere in presenza di una violazione dell'art. 2, par. 4. Nel caso di un attacco informatico, se rivolto ad un sistema considerato altamente sicuro, è molto probabile che esso rientrerà nella definizione di uso della forza;
5. la *misurabilità degli effetti*, che si sviluppa mediante un'analisi quantitativa e qualitativa degli effetti prodotti da un attacco; nel caso di un *cyber attack*, per essere questo qualificato quale attacco armato, dovrebbe produrre i medesimi effetti o danni di un attacco di tipo convenzionale;
6. la *presunzione di legalità*, che si stabilisce in base alla presenza o assenza di leggi che sanzionano l'azione in questione; qui, il problema principale sta proprio nell'assenza di leggi in ambito *cyber*. Ciò nonostante, gli Stati prima e il contesto internazionale poi stanno cercando di adattare i propri ordinamenti al mutare del contesto, oggi più tecnologico e interconnesso. La dimensione dei *cyber attack* si muove proprio all'interno di questo *vacuum* giuridico, che consente di realizzare attacchi informatici non sempre perseguibili dai diritti statuali interni ovvero dal diritto internazionale;

7. la *responsabilità dell'attacco*, che deve essere necessariamente imputabile ad uno Stato[98]. A riguardo, rimandiamo al paragrafo relativo alla responsabilità internazionale anticipando che nel *cyber space* la titolarità dell'attacco è uno degli elementi salienti che pone il diritto nazionale e internazionale nella difficoltà di individuare univocamente il responsabile di un attacco informatico, quasi mai attore statuale.

Ad ogni modo, questo approccio non è universalmente riconosciuto come valido; al contrario, l'analisi di Schmitt è stata criticata da altri studiosi in quanto troppo soggettiva e, di fatto, difficile da mettere in atto a causa della scarsità delle informazioni di cui nella realtà si è solitamente in possesso quando si verifica un attacco informatico.

Art. 39 ss.: l'uso della forza autorizzato dal Consiglio di Sicurezza

L'art. 39 della Carta delle Nazioni Unite permette al Consiglio di Sicurezza di intervenire ogni qualvolta si verifichi una violazione dell'art. 2, par. 4 della stessa.
Ad ogni modo, determinare che questo accada ha a che fare più con una decisione di tipo politico piuttosto che con una decisione di tipo giuridico. Questo dipende, soprattutto, dal meccanismo decisionale interno al Consiglio di Sicurezza che permette ai cinque membri permanenti di bloccare ogni delibera attraverso l'esercizio del proprio diritto di veto. Nato come misura per convincere tutte le più grandi potenze vincitrici al termine della Seconda Guerra Mondiale ad aderire all'Organizzazione delle Nazioni Unite, tale diritto si è trasformato in uno dei più grandi ostacoli che impediscono il buon funzionamento di questa organizzazione.
Ciò è stato evidente soprattutto nel periodo della Guerra Fredda, durante il quale entrambe le superpotenze in competizione (Stati Uniti e URSS) utilizzavano il potere di veto secondo i propri interessi nazionali; eppure simili azioni hanno avuto luogo anche nel periodo immediatamente successivo alla fine di questa: pensiamo, ad esempio, al caso del conflitto in Cecenia negli anni Novanta. Qui, erano in gioco gli interessi della Russia che ha esercitato il proprio potere di veto per evitare l'ingerenza di potenze esterne in una situazione che tale Paese riteneva rientrare nei propri affari interni.
Tale difficoltà è uno dei motivi in base ai quali molti hanno accusato le Nazioni Unite di essere un mero strumento nelle mani delle grandi potenze; tuttavia, occorre ricordare che non sempre è così e soprattutto che, in ogni caso, la costruzione di tale struttura permette un dialogo costante tra le nazioni e assicura la possibilità di prevenire o risolvere eventuali

[98] SCHMITT (2011: 569 ss.).

controversie e conflitti attraverso la cooperazione che gli Stati hanno assicurato di attuare prendendovi parte.

Proseguendo con la lettura della Carta delle Nazioni Unite, appare rilevante anche l'art. 41, che prevede la possibilità per il Consiglio di sicurezza di

> [...] decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

Dunque, esso può decidere quali misure, non implicanti l'uso della forza, debbano essere adottate per dare effetto alle sue decisioni, e può invitare i Membri delle Nazioni Unite ad applicare tali misure.
L'elenco delle misure che il Consiglio di sicurezza può adottare è soltanto un elenco esemplificativo; pertanto, questi può decidere di far adottare qualsiasi altra misura non implicante l'uso della forza che abbia scopo sanzionatorio, incluse quelle misure che possono aver a che fare con il *cyber* spazio (pensiamo, a titolo d'esempio, all'interruzione delle comunicazioni informatiche).
Infine, rilevante è l'art. 42 che, sebbene non abbia trovato applicazione negli anni, non ha perso la propria validità. Dunque, ai fini della nostra analisi può essere utile sapere che esso permette al Consiglio di sicurezza, una volta accertata l'esistenza di una minaccia alla pace, una violazione della pace o un atto di aggressione e qualora le misure non implicanti l'uso della forza si siano rivelate inadeguate, di autorizzare l'uso della forza con ogni azione necessaria per mantenere o ristabilire la pace e la sicurezza internazionale.
Appare, allora, auspicabile l'inserimento anche delle operazioni informatiche contro uno Stato o contro entità non statali all'interno di tali azioni.

A fronte di queste considerazioni, possiamo affermare che, in via teorica, il Consiglio di sicurezza avrebbe la piena autorità di far rientrare nella categoria di minaccia alla pace, se lo ritiene necessario, i *computer network attacks*[99], sebbene questo sino ad oggi non sia mai avvenuto. Esso ha, inoltre, l'autorità di intraprendere tali operazioni contro lo Stato o le entità non statali eventualmente oggetto di una risoluzione.
Ad ogni modo, dobbiamo tener conto delle caratteristiche del meccanismo decisionale interno al Consiglio di sicurezza e delle difficoltà che si riscontrano in termini giuridici rispetto alla qualifica degli attacchi informatici quali minaccia o uso della forza, al fine di essere consapevoli della sua potenziale incapacità di intervenire; più probabile, invece, sembra essere l'eventualità che uno Stato agisca da sé esercitando la legittima difesa.

[99] *Ivi*, p. 584.

Analizziamo, allora, nel dettaglio, cosa si afferma nella Carta delle Nazioni Unite all'art. 51.

Art. 51: la legittima difesa

Secondo l'art. 51 uno Stato può rispondere ad un attacco armato (sia che questo sia avvenuto sia nell'imminenza dello stesso) attraverso la cosiddetta legittima difesa. Da ciò deriva la conclusione in base alla quale uno Stato non può assolutamente esercitare il proprio diritto di legittima difesa se l'atto di cui si è vittima non raggiunge un livello tale da essere qualificato come attacco armato. Nel caso dei *cyber attacks* risulta, allora, fondamentale la loro identificazione quali minacce paragonabili ad un attacco armato di modo che ricorra il principio di legittima difesa.
La Carta delle Nazioni Unite non offre una specifica definizione di attacco armato; ciò nonostante, dal punto di vista giuridico possiamo affermare che un attacco armato è un atto illecito dal punto di vista del diritto internazionale[100], dal carattere transfrontaliero (e cioè commesso da uno Stato contro un altro Stato oppure da attori non statali contro uno Stato).
Esso implica necessariamente l'uso di un'arma ma, come la stessa Corte internazionale di giustizia ha affermato, non rileva la natura dell'arma impiegata.
Gli studiosi, dal canto loro, tenendo conto delle moderne tecniche di guerra, hanno elaborato diversi approcci per determinare se e quando un attacco raggiunge il livello richiesto per essere considerato un attacco armato.
Il primo approccio si focalizza sui mezzi impiegati per compiere l'attacco. Esso, tuttavia, si adatta molto bene ad un'analisi dei tradizionali strumenti di guerra ma risulta inapplicabile nel caso in cui vogliamo concentrarci su un attacco informatico: di fatto, gli strumenti tradizionali utilizzati dagli Stati durante i conflitti (bombe, missili o carri armati) possono essere definiti in base alle loro caratteristiche fisiche; lo stesso non possiamo fare in caso di *cyber attacks*.
Il secondo approccio guarda, invece, all'obiettivo dell'attacco: se un attacco colpisce un'infrastruttura critica di uno Stato sarà considerato un attacco armato a priori, al di là degli effettivi danni da questo prodotti. Per infrastruttura critica, come abbiamo visto nel precedente capitolo, si intende generalmente un sistema, una risorsa la cui distruzione, interruzione o momentanea indisponibilità indebolisce in maniera significativa l'efficienza o il funzionamento normale di un Paese[101]. Tale approccio, se applicato agli

[100] Sulla nozione di illecito internazionale vedasi Conforti (2014: 321-335).
[101] Solitamente sono associati al concetto di infrastrutture critiche le risorse idriche, il sistema di telecomunicazioni, i trasporti, le banche e i servizi finanziari o la sanità. Esistono diverse definizioni di infrastruttura critica.
A livello europeo, l'8 dicembre 2008 il Consiglio dell'Unione europea ha emanato la direttiva 2008/114/CE *relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione* che al punto a) dell'art. 2 fornisce una definizione sulla base della quale un'infrastruttura critica è "asset,

attacchi informatici, ci permetterebbe di estendere senza ombra di dubbio le previsioni della Carta delle Nazioni Unite a tutte quelle situazioni in cui un *cyber attack* è volto a colpire un'infrastruttura critica.
Il terzo approccio, condiviso da molti studiosi, si concentra invece sulle conseguenze e sugli effetti di un attacco. Questo approccio è stato elaborato partendo proprio dall'affermazione, sopra citata, della Corte internazionale di giustizia e considera armato un attacco solo se questo provoca la morte o il ferimento di un certo numero di vittime, la distruzione di certe aree o proprietà o di altri 'oggetti tangibili'. Si tratta di un approccio molto concreto che si distacca in maniera evidente dal precedente. Sulla base di questo, dovremmo concludere che, per essere considerato attacco armato, un *cyber attack* dovrà produrre i medesimi effetti di una classica operazione militare.
A prescindere dai tre approcci sopra menzionati, il nodo principale da sciogliere riguarda la sussistenza delle condizioni che assimilerebbero un *cyber attack* ad un attacco armato e questo per diverse ragioni.
La prima è che sino ad ora non si è mai verificato un attacco informatico, seppur grave, che sia stato in grado di causare quei danni (tipici di un attacco armato convenzionale) necessari affinché si possa parlare di uso della forza.
La seconda riguarda la difficoltà di individuare il responsabile dell'attacco e di accorgersi di essere effettivamente vittima di un attacco informatico per tempo, in modo da permettere l'esercizio del diritto alla legittima difesa. Il caso STUXNET[102] è, a riguardo, emblematico. In tale occasione né l'autore dell'attacco né la causa e i danni sono stati verificati se non dopo la fine dell'attacco stesso e, perciò, non è stato possibile rifarsi al diritto di legittima difesa. Questa condizione è ricorrente pressoché in tutte le circostanze riconducibili ad un attacco informatico proprio per l'immediatezza che, usualmente, lo caratterizza.
Diverso è il caso in cui un attacco informatico preceda la realizzazione di un attacco armato convenzionale. Riprendiamo il caso dell'attacco israeliano alla centrale nucleare siriana del 2007: in tale occasione, prima dell'attacco aereo Israele avrebbe realizzato un attacco informatico mirato a rendere inefficace la difesa aerea siriana falsando i dati rilevati dalla catena dei radar di scoperta. Cosa avrebbe potuto fare la Siria se si fosse accorta di ciò stava per accadere? Possiamo parlare di un diritto alla legittima difesa preventiva? L'interpretazione restrittiva della Corte internazionale di giustizia non sembrerebbe provare la legittimità di una legittima difesa preventiva.

---

system or part there of located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".
Nello stesso modo ha proceduto lo U.S Homeland Security Office, il quale descrive un'infrastruttura critica come l'insieme di "assets, systems and networks, both physical and digital, which are so important to the state that their incapacitation or destruction would have debilitating effect on security, national economic security, national public health or safety, or any combination thereof". [U.S. Office of Homeland Security, *"What Is Critical Infrastructure?"*, 2013, http://www.dhs.gov/].
[102] *Ivi*, pag. 11.

Secondo alcuni, tuttavia, non sarebbe necessario attendere che il nemico attacchi poiché uno Stato potrebbe difendersi nell'imminenza dell'attacco; in tal caso, deve ovviamente palesarsi la necessità dell'autodifesa immediata, senza che vi sia possibilità di riflessione alcuna[103]. Occorre, però, operare una distinzione tra l'ipotesi in cui un attore sta semplicemente acquisendo la capacità di avviare un attacco in futuro (in questo caso, verrebbe meno il criterio dell'immediatezza della risposta) e l'ipotesi in cui, invece, vi siano informazioni abbastanza certe da supporre che l'attore abbia già deciso di condurre un attacco (che può essere considerato, perciò, imminente).

Secondo altri, invece, in caso di attacchi informatici possono essere individuate due situazioni soltanto in cui possa essere fatto valere il diritto alla legittima difesa.
La prima prevede che un'operazione informatica preceda la minaccia di un attacco armato di tipo convenzionale; in tal caso, per stabilire se sorge il diritto alla legittima difesa ciò che si deve prendere in considerazione è l'obiettivo dell'attacco: se esso ha come bersaglio sistemi di allarme, postazioni radar o satellitari, comunicazioni militari o sistemi di emergenza è altamente probabile che uno Stato giudichi imminente un attacco convenzionale (ricordiamo nuovamente il caso siriano). Diversamente, un attacco a sistemi finanziari o mediatici generalmente non sembra preludere l'imminenza di un attacco convenzionale; tuttavia, qualora il contesto in cui ciò avviene sia caratterizzato da crescenti tensioni tra gli Stati allora è probabile che una delle parti possa ritenere che sia imminente anche la commissione di un attacco convenzionale.
La seconda riguarda, invece, la valutazione della gravità di un attacco informatico già verificatosi e la probabilità che ad esso ne segua un altro ancor più grave (tale da raggiungere effetti assimilabili a quelli di un attacco armato). Si tratta di un'ipotesi che fino ad oggi, come già detto, non ha ancora avuto un riscontro nella realtà; si crede che, in via generale, un attacco informatico non potrà mai produrre gli stessi danni prodotti dall'impiego di armi biologiche, nucleari o cinetiche e che, pertanto, il diritto all'autotutela in una situazione del genere non dovrebbe sussistere. Tuttavia, è bene che si lasci aperta questa possibilità ancorché essa non si sia ancora verificata.

Per concludere, quasi nessuno Stato al momento sembra voler consolidare l'idea di un'interpretazione più certa delle norme internazionali con riferimento alle operazioni informatiche e sembra prevalere, al contrario, una condotta non adeguatamente incisiva che garantisce sovente una maggiore libertà di azione. Eppure, tenuto conto dell'utilizzo sempre più frequente dei mezzi informatici e dell'incremento dei *cyber attacks*, è sempre più concreta la possibilità di un cambiamento di tendenza che potrà seguire due strade: il diritto esistente dei conflitti armati sarà a tutti gli effetti ritenuto applicabile

[103] SCHMITT (2013: 60).

anche alle operazioni informatiche (laddove gli Stati esprimano un *consensus* generale sulle modalità di applicazione dello stesso) oppure si formalizzerà un trattato internazionale *ad hoc* che provvederà a fornire un'interpretazione delle norme internazionali già esistenti più conforme al contesto cibernetico e a disciplinare le modalità di condotta di un'eventuale *cyber war*, similmente a quanto è stato fatto sino ad ora nell'ambito dei conflitti armati di stampo 'tradizionale'.
Nello specifico, le questioni rilevanti che tale trattato dovrà affrontare riguardano anzitutto il riconoscimento di un attacco informatico quale minaccia o uso della forza, di modo che il Consiglio di sicurezza abbia la possibilità, effettuate le dovute analisi del caso, di intervenire qualora si ritengano minacciate la sicurezza e la pace internazionali, nelle modalità già previste dalla Carta delle Nazioni Unite.
La seconda questione da affrontare riguarderà la definizione di attacco informatico quale attacco armato: si dovrà, dunque, chiarire quando questo possa essere considerato tale. A tal proposito, è necessario che gli Stati trovino un accordo circa i requisiti che permetterebbero di attribuire ad un *cyber attack* tale qualifica e le conseguenti modalità di risposta ad esso, consistenti anche in ulteriori operazioni informatiche.
Infine, qualora i membri della Comunità internazionale dovessero trovarsi d'accordo, si potrebbero definire nuove norme in materia affrontando questioni già trattate dal diritto internazionale umanitario. In tal caso, operando sempre un forte adattamento al contesto cibernetico, si potrebbero specificare i casi in cui un attacco informatico, che abbia causato gravi danni o persino vittime, sia da considerarsi un illecito internazionale. Ancorché sino ad oggi non si sia mai verificato alcun attacco informatico di tale portata, di fatto non possiamo escludere che tale ipotesi possa essere presa in considerazione in futuro e disciplinata da norme scritte.

Ad ogni modo, la strada è ancora lunga e al momento gli Stati sembrano preferire anzitutto agire all'interno del proprio territorio, mediante politiche di *cyber security* mirate e, in secondo luogo, dare vita a regimi di cooperazione internazionale non ancora orientati, però, verso la definizione di un unico sistema centralizzato di prevenzione e repressione degli attacchi informatici né alla definizione di una disciplina normativa chiara in materia.

2.4 Il regime di responsabilità internazionale

In questo paragrafo analizzeremo il concetto di responsabilità internazionale ed esamineremo le condizioni alla base della sua invocabilità per capire se e quando questa possa entrare in gioco in caso di *cyber attacks*.
Innanzitutto, diamo una definizione di responsabilità internazionale. Per responsabilità internazionale si intendono quelle relazioni giuridiche che vengono ad esistere in conseguenza della commissione di un fatto illecito secondo le regole di diritto internazionale, come specificato nell'art. 1 del *Progetto di articoli sulla responsabilità internazionale dello Stato*, adottato dalla Commissione di Diritto Internazionale che recita: "Every internationally wrongful act of a State entails the international responsibility of that State".
Tali relazioni consistono, di norma, in un rapporto giuridico tra lo Stato autore dell'illecito e lo Stato leso.
Il primo ha l'obbligo di effettuare una riparazione; il secondo ha il diritto di pretenderla e di comminare una contromisura nei confronti dello Stato autore dell'illecito.
Evidenziamo che nel diritto internazionale la responsabilità, al contrario di quanto accade nel diritto interno ove si distingue tra responsabilità civile e responsabilità penale, è una e una soltanto. Essa è disciplinata dal diritto internazionale consuetudinario, sebbene vi siano stati diversi tentativi di codificazione a partire dagli anni Cinquanta. Esiste, per l'appunto, il *Progetto di articoli della Commissione di diritto internazionale*, sopra citato, adottato nel 2001 e considerato in parte dalla Corte internazionale di giustizia come dichiarativo del diritto consuetudinario[104]; in questo paragrafo faremo riferimento ad alcuni articoli ivi contenuti.
Abbiamo detto che la responsabilità internazionale entra in gioco al momento della commissione di un fatto illecito, ma cosa si intende nel diritto internazionale per fatto illecito? Secondo l'art. 2 del Progetto, gli elementi distintivi di un illecito internazionale sono due:

- l'elemento oggettivo, che consiste nella condotta (omissiva o commissiva) contraria ad una norma di diritto internazionale; a riguardo è importante sottolineare che non rileva la natura della norma violata.
- l'elemento soggettivo, vale a dire l'accertamento che tale condotta sia imputabile ad uno Stato.

Per quanto riguarda il secondo elemento diverse sono le ipotesi per cui una determinata azione o omissione è imputabile ad uno Stato.

[104] RONZITTI (2013: 378).

In primo luogo, è imputabile ad uno Stato la condotta di un suo organo. In questo caso, si parla sia degli organi del potere esecutivo sia di quelli del potere legislativo e giudiziario[105].
La Corte internazionale di giustizia ha, tuttavia, elaborato una teoria (la cosiddetta teoria dell'*effective operational control*) in base alla quale sono equiparabili ad organi dello Stato anche le persone non dotate di tale qualifica nel diritto interno, purché si dimostri che lo Stato ritenuto responsabile eserciti su di esse un significativo grado di controllo che dia luogo ad una relazione di completa dipendenza tra l'agente e lo Stato[106].
Una diversa interpretazione della nozione di 'controllo' da parte di uno Stato su un gruppo di individui è stata fornita, invece, dal Tribunale Internazionale per la Jugoslavia: esso ha sancito il concetto di *'overall control*', espressione con la quale si vuole indicare l'insieme di atti mediante i quali uno Stato non soltanto supporta un gruppo di privati ma ne organizza e coordina le attività[107]. Stiamo parlando, dunque, di un controllo più globale che non sottende però un rapporto di completa dipendenza dallo Stato stesso e questa è la grande differenza tra le due interpretazioni in merito. La Commissione di diritto internazionale ha rifiutato, invece, tale accezione optando per la teoria secondo cui il controllo deve essere effettivamente esercitato su ogni specifico atto lesivo[108].
Nel *Progetto di articoli* si afferma, inoltre, che si possono considerare organi statali le persone o gli enti comunque sprovvisti di tale qualità in base al diritto interno dello Stato solo ove essi siano abilitati da questo ad esercitare prerogative dell'autorità di governo ed agiscano in tale qualità[109].
Al di là di queste ipotesi, normalmente la condotta di semplici individui non è imputabile ad uno Stato, a meno che la condotta di uno o più privati non venga fatta propria da questo, come è accaduto nel noto caso degli ostaggi a Teheran[110]. Soltanto in tale circostanza, dunque, lo Stato risponde direttamente della condotta di un individuo.

---

[105] Per quanto riguarda la loro qualità, ad ogni modo, si deve far riferimento al diritto interno.
[106] Sentenza della Corte internazionale di giustizia del 26 febbraio 2007 nel caso relativo *all'applicazione della Convenzione per la prevenzione e la repressione del crimine di genocidio (Bosnia and Herzegovina c. Serbia and Montenegro)*.
[107] *Progetto di articoli sulla responsabilità internazionale dello Stato, 2001*, art. 8: "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct".
[108] *Progetto di articoli sulla responsabilità internazionale dello Stato, 2001*, art. 8, commentario.
[109] *Progetto di articoli sulla responsabilità internazionale dello Stato*, 2001, art. 5: "The conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance".
[110] Il 4 novembre 1980, pochi mesi dopo la Rivoluzione islamica guidata dall'ayatollah Ruhollah Khomeini in Iran, diverse centinaia di studenti attaccarono l'ambasciata statunitense e presero in ostaggio 53 dei suoi dipendenti. La liberazione degli ostaggi avvenne solo il 20 gennaio 1981, al termine di lunghi negoziati. In tale occasione gli organi statali iraniani

Infine, un'ultima ipotesi prevede che, qualora un organo sia messo a disposizione di un altro Stato, la sua condotta lesiva sarà imputabile allo Stato a disposizione del quale è posto[111].

Dunque, abbiamo dato una definizione di illecito internazionale ed esaminato i casi in cui una condotta lesiva è imputabile ad uno Stato.
È necessario adesso analizzare anche quei casi in cui l'azione compiuta da un soggetto rimane di per sé contraria al diritto internazionale ma, intervenendo una circostanza particolare, viene meno la sua illiceità.
Stiamo parlando dei casi in cui si presenta una cosiddetta causa di esclusione dal fatto illecito. Sulla base della prassi sono state individuate, infatti, talune circostanze che, una volta verificatesi, escludono la responsabilità dello Stato per la commissione di un illecito internazionale.
Esse sono:

a) il consenso dell'avente diritto, che opera in relazione a qualsiasi violazione del diritto internazionale ad esclusione delle norme imperative[112] (il c.d. *jus cogens*);
b) la legittima difesa, che opera in relazione al divieto generale dell'uso della forza, diventato ormai norma di diritto generale;
c) le contromisure, lecite come reazione all'atto illecito compiuto dallo Stato nei cui confronti sono comminate. Esse possono consistere nella violazione di norme di diritto internazionale pattizio o consuetudinario;
d) la forza maggiore, dovuta al sopravvenire di una forza irresistibile o un avvenimento imprevedibile che rendono materialmente impossibile agire in conformità dell'obbligo;
e) lo Stato di necessità, per cui devono sussistere due condizioni.
   La prima prevede che l'atto necessitato debba essere il solo mezzo per salvaguardare un interesse essenziale di fronte ad un pericolo grave ed imminente.
   La seconda prevede che l'atto necessitato non comprometta gravemente un interesse essenziale dello Stato o degli Stati nei cui confronti l'obbligo è dovuto o della Comunità Internazionale nel suo insieme[113].

---

avallarono e approvarono la condotta degli studenti islamici di fatto divenuta imputabile allo Stato stesso.
[111] *Ivi*, art. 6.
[112] Vale a dire norme di diritto internazionale generale riconosciute ed accettate dalla Comunità internazionale nel suo insieme come inderogabili.
[113] RONZITTI (2013: 386-388).

Le conseguenze del fatto illecito

Dalla commissione di un illecito internazionale scaturisce un insieme di conseguenze a carico dello Stato offensore.
Tradizionalmente, tali conseguenze consistevano nell'obbligo dell'autore dell'illecito di effettuare la riparazione e nel diritto dello Stato leso di comminare una contromisura che aveva, secondo alcuni, uno scopo afflittivo (tipicamente essa consisteva nella rappresaglia), mentre, secondo altri, doveva essere volta ad ottenere l'esecuzione della riparazione.
All'interno del Progetto di articoli della Commissione di diritto internazionale troviamo una serie di conseguenze più complesse.
Oltre al dovere per l'autore dell'illecito di conformarsi agli obblighi derivanti dall'illecito, questi deve adempiere ai seguenti obblighi:

- cessazione dell'illecito, se siamo in presenza di un illecito a carattere continuativo;
- garanzia di non reiterazione dell'atto in questione;
- riparazione del danno, sia materiale sia morale, che può assumere la forma della restituzione (attraverso la quale si ristabilisce lo *status quo ante*, cioè la situazione preesistente la commissione dell'illecito); del risarcimento, dovuto quando la restituzione non è materialmente possibile o non riesca a riparare integralmente il danno (in tal caso, la somma a titolo di risarcimento deve coprire ogni danno suscettibile di valutazione economica); infine, della soddisfazione, la quale va a riparare invece i danni di natura morale attraverso scuse formali o manifestazione di rincrescimento.

Cyber attacks e regime di responsabilità internazionale

Ai fini della nostra analisi risulta fondamentale capire se, nel caso dei *cyber attacks*, sia possibile imputare tali atti a un ente preciso e se, ove questo risulti essere uno Stato o avere un legame con questo, siamo nella condizione di poter invocare il regime di responsabilità internazionale.
Stabilire se un atto sia riconducibile ad uno Stato richiede una procedura che consta di diverse fasi.
Occorre, innanzitutto, risalire alla fonte d'origine dell'attacco; in secondo luogo, identificare l'individuo o il gruppo di individui che hanno perpetrato l'attacco e, infine, individuare un collegamento tra l'ideatore dell'attacco e, eventualmente, uno Stato.
Tale processo si caratterizza per una simultanea presenza di elementi tecnici, politici e giuridici.
Per quanto riguarda gli aspetti tecnici, facciamo riferimento al processo di identificazione forense riguardante la fonte dell'attacco informatico, che può offrire una più o meno certa geo-localizzazione del dispositivo dal quale l'attacco ha avuto origine. In questo modo, si può risalire al luogo in cui si

trovava, probabilmente, chi ha dato avvio all'attacco o quanto meno il dispositivo dal quale esso è partito. Tuttavia, tale procedura non permette l'identificazione del responsabile. Quest'obiettivo viene perseguito, invece, mediante una sempre più frequente collaborazione con i servizi di intelligence, la quale genera uno scambio con le autorità di tutte quelle informazioni che essi sono in grado di raccogliere ed analizzare col fine di tracciare un profilo dell'autore dell'attacco, scoprire le sue abilità e le sue intenzioni ed infine risalire ad eventuali legami con uno Stato o con altri enti. È in questo frangente che emerge l'aspetto per lo più politico del processo di imputabilità di un atto ad uno Stato.
Per ciò che concerne, invece, l'aspetto legale rilevano le norme di diritto internazionale in materia.
Esaminiamo, allora, la questione dell'imputabilità di un atto ad uno Stato.
Adottiamo come punto di partenza il caso dell'Estonia del 2007 e focalizziamoci sulle accuse mosse nei confronti della Russia, considerata l'artefice e l'ideatrice della serie di attacchi verificatisi. Più precisamente, l'Estonia considerava responsabile degli attacchi l'organizzazione nazionalistica russa RBN (Russian Business Network). Questa, tuttavia, non è identificabile come un organo statale né come un ente dipendente dal governo russo. Secondo quanto affermato precedentemente potremmo far leva sull'idea per cui se vi è un '*overall control*' dello Stato, laddove l'attacco sia perpetrato da privati o comunque non da organi di uno Stato, l'atto è imputabile ad esso. Tuttavia, nel caso specifico, non sono state rinvenute prove sufficienti per poter affermare che la Russia abbia esercitato il proprio controllo sugli autori dell'attacco né che abbia ufficialmente preso parte alla pianificazione delle operazioni, nonostante sia stata rilevata una partecipazione del Paese. Appare evidente, allora, la difficoltà che emerge in caso di *cyber attacks* relativa, innanzitutto, all'identificazione dei responsabili dell'attacco e, in seconda battuta, alla raccolta delle necessarie prove che attestino un eventuale legame con uno Stato di modo che possa essere invocato il regime di responsabilità internazionale[114].
Ciò detto, però, sulla base della prassi e della giurisprudenza internazionali possiamo tentare di stabilire quando effettivamente la commissione di un attacco informatico o il suo sostegno possano essere considerati un illecito internazionale imputabile ad uno Stato.
Consideriamo, *in primis*, l'ipotesi in cui un attacco informatico abbia origine da un'infrastruttura governativa; si tratta di un organo statale o che comunque agisce in nome di uno Stato, pertanto secondo il diritto internazionale qualsiasi azione da questi commessa è imputabile a questi. Tuttavia, il fatto che l'attacco provenga da un'infrastruttura statale, sebbene attesti senza dubbio un legame con uno Stato, non è di per sé condizione sufficiente a dimostrare la sua responsabilità in merito al fatto illecito compiuto. Questo è vero poiché è possibile che la stessa infrastruttura sia stata già oggetto di un attacco da parte di *hackers* che, una volta acquistatone

[114] BUCHAN, ROSCINI, TSAGOURIAS (2014: 4 ss.).

il controllo, hanno sferrato un ulteriore attacco puntando su un altro obiettivo. Peraltro, operazioni di questo tipo non si limitano alle infrastrutture presenti sul territorio di uno Stato ma possono riguardare anche le navi, i velivoli e i satelliti di un Paese. Occorre, dunque, sempre indagare sui fatti per accertare l'eventuale responsabilità di uno Stato anche laddove, secondo le regole internazionali, apparentemente la responsabilità conseguente la commissione di un atto illecito sembrerebbe molto semplice da attribuire ad esso.

Una seconda riflessione che possiamo fare scaturisce dall'affermazione per cui un illecito internazionale possa consistere sia in una condotta commissiva che omissiva. Ricordiamo il caso del canale di Corfù[115], nel quale la Corte internazionale di giustizia stabilì che l'Albania era a conoscenza, o quanto meno avrebbe dovuto essere a conoscenza, della presenza di mine nel canale di Corfù e che fosse, pertanto, suo dovere avvertire gli altri Stati di modo che nessuno venisse colpito[116] (come invece è accaduto). Attraverso questa lettura della vicenda, la Corte ha così stabilito che la condotta omissiva del Paese aveva integrato un illecito internazionale.

Tale caso è rilevante per la nostra analisi poiché ci consente di affermare che uno Stato, consapevole del fatto che il suo territorio o le sue reti di informazione vengano utilizzati (da un altro Stato o da un gruppo di attori privati) per compiere attività illecite di *cyber warfare* contro un altro Stato o altri Stati, può essere ritenuto, senza alcun dubbio, responsabile della commissione di un illecito internazionale qualora non attui misure sufficienti a prevenire tali attacchi o non dia avviso di quanto sta accadendo. Nondimeno, potrebbero verificarsi circostanze tali per cui uno Stato può non essere in grado di prevenire che un attacco venga lanciato o avvisare un altro Stato a causa della scarsità delle informazioni in suo possesso riguardanti la fonte d'origine dell'attacco, il momento esatto in cui esso sarà lanciato o il *target* di riferimento. In tal caso, spetterebbe ad un organo, quale ad esempio la Corte internazionale di giustizia, analizzare il susseguirsi degli eventi e stabilire se esistano o meno le condizioni per far scattare la responsabilità internazionale dello Stato in questione.

---

[115] Si fa riferimento, nello specifico, al complesso di incidenti verificatisi nel 1946 nel canale di Corfù (alla frontiera marittima tra Grecia e Albania) che videro coinvolte delle unità della *Royal Navy* britannica. Nel primo incidente, avvenuto il 15 maggio 1946, due incrociatori della *Royal Navy* in navigazione nel canale furono cannoneggiati, senza essere colpiti, da batterie costiere della Repubblica Popolare Socialista d'Albania, che accusava i britannici di essere entrati nelle sue acque territoriali. Il 22 ottobre 1946, invece, una formazione britannica in navigazione nel canale finì in un campo di mine navali non segnalato, riportando gravi danni. Infine, tra il 12 e il 13 novembre 1946 forze navali britanniche tornarono nel canale per bonificare il tratto minato che aveva causato l'incidente del 22 ottobre, sconfinando nelle acque territoriali dell'Albania e causando forti proteste da parte del governo albanese.
L'incidente causò una grave crisi diplomatica tra Londra e Tirana; il caso venne portato all'attenzione della Corte internazionale di giustizia, la cui sentenza resa il 9 aprile 1949, costituì un importante precedente nella definizione di alcuni principi fondamentali del diritto del mare e del diritto internazionale.

[116] Sentenza della Corte internazionale di giustizia del 9 aprile 1949 nel caso dello *Stretto di Corfù (Albania c. Regno Unito)*.

Egualmente importante, dato l'alto numero di attori privati all'interno del *cyber space*, risulta la tesi (già evidenziata nel caso degli ostaggi a Teheran) per cui una condotta di privati può essere imputabile ad uno Stato qualora esso la faccia propria. Da ciò ne discende che qualsiasi attività di *cyber warfare* intrapresa da privati, se fatta propria da uno Stato, è imputabile a quello Stato. Lo stesso vale per le agenzie private o governative che si comportano di fatto come organi dello Stato poiché agiscono su istruzione o sotto la direzione o il controllo di questo. Ricordiamo, però, che la dottrina sposa la tesi secondo cui il controllo dello Stato debba effettivamente essere esercitato su ogni atto lesivo.
Nell'era contemporanea, questo tipo di ipotesi non è così lontana dalla realtà. Spesso gli Stati si avvalgono dell'aiuto di agenzie di privati (le cosiddette *private corporations*) conferendo loro un'autorità di governo per condurre operazioni di tipo difensivo o di tipo offensivo all'interno dello spazio cibernetico. Gli Stati Uniti sono stati tra i primi Paesi a ricorrere a società private: è il caso della EC-Council, a cui si è ricorsi per far acquisire al proprio personale dell'US Navy, FBI, CIA e US Army le certificazioni necessarie al contrasto delle forme più sofisticate di *cyber attacks*[117]. Anche il Regno Unito ha attuato misure in tal senso. Ad esempio, nel 2012 il ministro del *Foreign Office* nel Regno Unito ha annunciato un programma per l'arruolamento di 100 specialisti informatici per il GCHQ (*Government Communications Head Quarter*), l'MI5 e l'MI6 (ossia i servizi segreti britannici), rivolto a giovani laureati in Scienze, Tecnologie e Ingegneria e persino di esperti di *computer-game*[118]. Tra le attività intraprese da queste agenzie ricordiamo le più frequenti ossia quelle di *cyber intelligence*, *cyber espionage* ma anche quelle che prevedono veri e propri *cyber attacks* alle infrastrutture critiche di uno Stato. Infatti, il furto di informazioni top secret, commerciali e industriali, la violazione di dispositivi tecnologici per il prelevamento di database e messaggistica hanno visto un notevole incremento negli ultimi anni.

In conclusione, possiamo affermare che il diritto internazionale offre già un quadro normativo ipoteticamente applicabile al caso dei *cyber attacks*, quanto meno in relazione alla probabilità che un attacco, sia pur perpetrato da privati, sia imputabile ad uno Stato. Il problema, come già in parte accennato durante la discussione degli attacchi verificatisi nel 2007 in Estonia, è che non sempre risulta semplice individuare chi ha perpetrato l'attacco e soprattutto rinvenire poi un collegamento con uno Stato. Inoltre, data la trans-nazionalità che spesso caratterizza i *cyber attacks* è sempre più difficile per uno Stato rivalersi su un altro.
Nel prossimo paragrafo, analizzeremo la questione alla luce del rispetto del principio di sovranità per definire i casi in cui è possibile perseguire i

[117] TETI (2013: 97).
[118] *Ivi*, p. 98.

criminali informatici anche laddove questi abbiano agito al di fuori del territorio dello Stato nel quale l'attacco ha luogo.

2.5 Principio di sovranità territoriale, responsabilità internazionale e *cyber attacks*

Prima di procedere con la nostra analisi, rivediamo in breve la definizione di Stato secondo il diritto internazionale e l'importanza del principio di sovranità territoriale.
Gli Stati sono definiti dal diritto internazionale come degli enti caratterizzati da due elementi principali: la sovranità e l'indipendenza. Ciò significa che ogni Stato esprime la propria autorità e i propri poteri di governo su un territorio e sui soggetti ad esso appartenenti ed è indipendente nei confronti degli altri Stati.
Nel diritto costituzionale, lo Stato viene definito come un ente '*superiorem non recognoscens*' (che non riconosce un altro superiore). Si tratta di una formula latina che si riferisce, in particolar modo, ai supremi organi dello Stato che, posti in posizione di indipendenza e parità innanzitutto tra di loro, non sono sottoposti, poi, ad alcun potere superiore.
Nelle relazioni internazionali, e nel diritto internazionale, il principio di sovranità territoriale è un principio molto importante che si riferisce alla capacità dello Stato di esercitare il proprio *imperium* in maniera esclusiva all'interno del suo territorio. Tale principio viene salvaguardato dal diritto internazionale attraverso la garanzia offerta dal divieto di ingerenza negli affari interni di uno Stato (divieto che persino le Nazioni Unite devono rispettare[119]); esso protegge, inoltre, l'integrità territoriale di uno Stato mediante la proibizione della sottrazione di parti del suo territorio (senza una valida giustificazione).
Occorre, tuttavia, specificare che oggetto della sovranità territoriale sono, non soltanto il territorio di uno Stato in senso stretto, ma anche il mare territoriale e lo spazio aereo sovrastante; è preferibile, dunque, utilizzare il termine giurisdizione per indicare i confini all'interno dei quali uno Stato esercita la propria autorità.
A tal proposito, ad esclusione dei limiti imposti dal diritto internazionale riguardanti il trattamento che deve essere riservato agli Stati stranieri, ai loro organi e ai loro cittadini nonché il trattamento da riservare ai propri cittadini, lo Stato è libero di assoggettare alla disciplina che più gli conviene i rapporti che si svolgono all'interno della propria giurisdizione. Questa sfera di competenza statale viene denominata *domestic jurisdiction* (o dominio riservato) e viene protetta dalle norme internazionali, come prima citato, mediante il divieto di ingerenza negli affari interni di uno Stato. Qui, il ruolo della Corte internazionale di giustizia è stato fondamentale. Essa ha, infatti, provveduto a precisare quali sono le materie oggetto del dominio riservato di uno Stato nel caso *Nicaragua c. Stati Uniti*. Queste sono la determinazione

[119] "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction ion of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.", art. 2, par. 7, Carta delle Nazioni Unite, San Francisco, 1945.

del sistema politico, economico, sociale e culturale e la formulazione della politica estera[120].

Con l'inizio del XX secolo abbiamo assistito, tuttavia, ad una progressiva erosione del principio di sovranità, determinata in parte dalla globalizzazione economica e in parte dall'estensione della tutela internazionale dei diritti umani.
L'introduzione delle reti informatiche ha, poi, definitivamente eliminato il concetto di confine territoriale di uno Stato permettendo, di fatto, un abbattimento di tutte le barriere che separavano i vari popoli del mondo.
Il concetto di frontiera non ha, infatti, alcuna rilevanza nel c.d. *cyber* spazio così come il concetto di sovranità territoriale. Questo perché il *cyber* spazio fa riferimento ad una dimensione immateriale, anche se per accedervi occorrono oggetti fisici quali computer, *server* o *routers*.
Di per sé il *cyber* spazio costituisce, quindi, un spazio virtuale senza confini, che mette in comunicazione i computer di tutto il mondo in un'unica rete permettendo ai diversi utenti di interagire tra loro. Se, da un lato, ciò costituisce un vantaggio, dall'altro è proprio il vasto numero di attori presenti in rete a scalfire la capacità degli Stati di esercitare un certo grado di controllo su ciò che accade all'interno della propria giurisdizione. Questi, infatti, possono regolamentare tutto ciò che riguarda le infrastrutture informatiche, in parte i contenuti in rete ma certamente non possono esercitare il proprio controllo su tutti gli utenti e su come essi agiscono in essa (specialmente se questo si verifica al di fuori della propria giurisdizione).
Consideriamo, ad esempio, il fatto che un *hacker* possa fisicamente operare in un Paese, manipolare i dati di un sistema informatico di un altro e muoversi all'interno del *cyber* spazio senza incontrare ostacolo alcuno a tal punto che le conseguenze prodotte dalle sue azioni possono colpire chiunque e ovunque. Si potrebbe affermare che uno Stato possa in ogni caso reclamare la propria giurisdizione quando l'attacco ha effetti sul proprio territorio; tuttavia, occorre considerare innanzitutto la tipologia d'attacco, la fonte d'origine dell'attacco e soprattutto se questo ha avuto effetti soltanto nel territorio di uno Stato oppure di più Stati. Un ulteriore problema si pone se la nazionalità dei responsabili è diversa da quella dello Stato oggetto di attacco. In base a quali criteri possiamo decidere qual è lo Stato competente a giudicare? Si potrebbe pensare di ritenere competente lo Stato nel quale, ad esempio, un virus è stato introdotto oppure lo Stato o gli Stati i cui sistemi sono stati infettati dal virus stesso o ancora lo Stato o gli Stati nei quali si sono riflesse le conseguenze dell'attacco. Le possibilità sono diverse.
La strada della cooperazione, mediante la conclusione di trattati internazionali o l'elaborazione di nuove norme consuetudinarie, sembra

[120] Sentenza della Corte internazionale di giustizia del 27 giugno 1986 nel caso delle *Attività militari e paramilitari degli Stati Uniti in Nicaragua e contro il Nicaragua (Nicaragua c. Stati Uniti)*.

allora la via più adeguata per superare questi ostacoli. Mediante tale procedura si avrebbero regole più chiare e definite.
Uno degli strumenti che al momento ben si adatta ad essere impiegato per perseguire i criminali informatici (i cui atti, invece, non risultano imputabili ad uno Stato) è quello dell'estradizione, alla cui base vi è in genere proprio un accordo tra gli Stati al fine di garantire la consegna da parte di uno Stato ad un altro dei responsabili di un atto penalmente perseguibile, che si trovano all'interno della giurisdizione del primo ma che saranno giudicati e, nel caso, condannati nel secondo. Si tratta di uno strumento che permetterebbe di agire, in collaborazione con gli altri membri della comunità internazionale, in maniera efficace in un contesto, come quello del *cyber space*, che sfugge al concetto di giurisdizione.
Certo è che, comunque, si tratta sempre di strumenti richiedono basati sulla volontà degli Stati a collaborare, essendo essi vincolanti soltanto nei confronti di chi decide di prendervi parte.
Ad ogni modo, al momento i trattati già esistenti che disciplinano l'estradizione (sia a livello bilaterale sia a livello multilaterale) sembrano potersi applicare anche nel caso di *cyber crimes* o *attacks:* non vi sono difficoltà a riguardo se non che devono essere soddisfatte due condizioni.
La prima prevede che il crimine che si persegue deve essere tale in entrambi gli Stati. Questa è forse la questione di maggior rilievo perché, come abbiamo già avuto modo di dire, non tutti gli Stati hanno adottato norme di *cyber security* o non tutti seguono gli stessi standard, soprattutto in relazione alla qualificazione di un atto quale crimine informatico.
La seconda stabilisce la necessità per cui tali azioni siano inserite tra i cosiddetti reati estradabili.
È importante sottolineare, altresì, che le norme in materia di estradizione hanno come obiettivo anche quello di assicurare comunque il rispetto del principio di sovranità. Prendiamo come esempio l'art. 4 della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, nel quale si afferma che

> States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States[121] [e che nulla in tale Convenzione] entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

Di fatti, come anche risulta essere secondo il diritto internazionale consuetudinario, uno Stato non può interferire negli affari interni di un altro Stato e perciò controllare i suoi cittadini, nonostante il fatto che questi possano, ad esempio, compiere un crimine o un attacco informatico nei suoi confronti. Esso può, però, instaurare un rapporto di cooperazione con gli altri

[121] Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, Palermo, 15 Novembre 2000.

Stati per perseguire eventuali reati anche laddove l'autore dell'illecito non si trovi nel suo territorio.
Ricordiamo comunque che, essendo un mondo virtuale, il *cyber space* non è soggetto alla sovranità di alcuno Stato. Tuttavia, è corretto affermare che ogni Stato può esercitare il proprio controllo sulle infrastrutture informatiche e le attività associate ad esse. Ciò significa che:

1. le infrastrutture informatiche sono sottoposte al controllo legale di uno Stato;
2. la sovranità territoriale di uno Stato ha funzione di 'protezione' nei confronti di tali infrastrutture, sia nel caso in cui queste siano di dominio pubblico e sia nel caso in cui queste appartengano a privati. Riprendendo quanto affermato sopra, perciò, nessun altro Stato al di fuori di quello ove tali infrastrutture si collocano ha la facoltà di intervenire contro di esse o di attaccarle con l'obiettivo di danneggiarle o distruggerle se non violando il principio di sovranità commettendo, dunque, un illecito internazionale)[122];
3. il principio di sovranità territoriale consente agli Stati di imporre eventuali restrizioni d'accesso a Internet (sebbene a riguardo occorre tener conto delle norme internazionali a tutela dei diritti umani e delle condizioni da rispettare affinché tali restrizioni non siano illecite. La questione sarà approfondita nel terzo capitolo).

Ciò detto, dobbiamo pur sempre ricordare le difficoltà legate alla determinazione della fonte di un attacco informatico, dell'identità dei responsabili e del loro eventuale legame con uno Stato: è certamente comprensibile quanto arduo possa essere invocare il regime di responsabilità internazionale in tali casi, così come sarebbe difficile chiedere una collaborazione da parte di un altro Stato se non si è conoscenza del luogo in cui si trovano i responsabili di un attacco o se non si conosce la loro identità e provenienza.
Quello di cui si ha bisogno sono, dunque, informazioni e prove. Questo è stato sancito anche dalla stessa Corte di giustizia internazionale, sempre nel caso *Nicaragua c. Stati Uniti*, nel quale si è evidenziato che uno dei problemi inerenti all'applicazione del regime di responsabilità internazionale non consisteva nell'incapacità di imputare particolari azioni ad uno Stato ma nella scarsa presenza di prove riguardanti l'identità di chi aveva compiuto quelle azioni[123]. Perciò, chi è vittima di un attacco informatico deve dapprima raccogliere tutte le prove necessarie a dimostrare la colpevolezza di un soggetto, privato o pubblico, in base al principio secondo cui l'onere della prova è a carico di chi fa valere in giudizio un diritto (*onus probandi incumbit actori*); questo lo può fare attraverso dichiarazioni ufficiali, testimonianze e prove tecnicamente valide che attestino l'identità e la

[122] SCHMITT (2013: 16 ss.).
[123] *Ibidem.*

responsabilità di chi ha commesso l'attacco. Ottenere le prove, tuttavia, non è così semplice e spesso, ancora una volta, sarebbe necessaria la collaborazione con altri Stati. Non sempre questa ha luogo, soprattutto a causa della scarsa attenzione di alcuni Paesi per la *cyber security*, la non omogeneità delle legislazioni nazionali e, spesso, la mancanza totale di un quadro legale che reprima e persegua certe attività informatiche.
Infine, teniamo conto che per quanto riguarda la capacità e il dovere di uno Stato di prevenire la commissione di crimini nel proprio territorio o quanto meno avvisare gli altri Stati di quanto sta accadendo (come la Corte internazionale di giustizia ha provveduto a raccomandare), ricordiamo che spesso questo risulta impossibile da realizzare efficacemente a causa della mancanza di dettagliate informazioni a riguardo.

Consideriamo, ora, il caso in cui sia stata accertata la responsabilità di uno Stato per la commissione di un attacco informatico: secondo il diritto internazionale, a questo punto, lo Stato leso ha il diritto di chiedere immediatamente una riparazione e di intraprendere delle contromisure, in risposta all'attacco subìto. Sembra al momento possibile rispondere ad un attacco ricorrendo persino a contromisure in ambito *cyber* purché si rispettino però i requisiti stabiliti dal diritto internazionale a riguardo: tali contromisure dovranno:

- avere carattere pacifico, in modo da non violare l'art. 2 par, 4 della Carta ONU;
- rispettare il criterio della proporzionalità rispetto alla lesione subita, come stabilito dall'art. 49 del *Progetto di articoli* redatto dalla Commissione di diritto internazionale. Questo perché l''effetto della contromisura non deve essere manifestamente sproporzionato rispetto alla gravità dell'illecito internazionale commesso;
- rispettare le norme di *jus cogens* e di diritto umanitario.

Ad ogni modo, adottare contromisure significherebbe adottare un approccio di difesa attiva, che potrebbe ingenerare una *escalation* degli eventi; una migliore opzione potrebbe consistere nella realizzazione di strategie di difesa passiva, in grado di impedire o vanificare gli effetti di un attacco piuttosto che dovervi reagire[124].

Abbiamo, perciò, fornito una breve analisi della nuova dimensione che ha assunto il conflitto internazionale, ossia la cosiddetta *cyber war*, al fine di individuare quali operazioni condotte nello spazio cibernetico sono riconducibili a tale nozione e di esaminare le norme internazionali vigenti nell'ambito dei conflitti armati con lo scopo di vedere se e come è possibile applicarle a questa moderna forma di conflittualità.

[124] SETTI (2017: 9 ss.).

La difesa del *cyber* spazio non riguarda, tuttavia, soltanto l'ambito militare ma, come abbiamo visto nel primo capitolo, anche l'ambito civile.
Il mondo della *cyber security* è sempre più legato sia alla nozione di sicurezza nazionale sia al tema della sicurezza dei dati e della tutela dei diritti umani in rete.
Nel prossimo capitolo esamineremo nel dettaglio questi aspetti, concentrando la nostra attenzione sulle strategie elaborate per affrontare la minaccia cibernetica e tenendo contemporaneamente conto anche dell'esigenza di proteggere gli individui soprattutto da tutte quelle *cyber operations* (attuate da privati o dagli Stati stessi) che ledono i diritti fondamentali di cui sono titolari.

CAPITOLO III

TUTELA DEI DIRITTI UMANI NELL'AMBITO DELLA *CYBER SECURITY*

In questo capitolo esploreremo il fenomeno di Internet ponendo la nostra attenzione sulla necessità di garantire anche all'interno del *cyber space* la tutela dei diritti e delle libertà fondamentali dell'uomo.
Internet è certamente il mezzo di comunicazione che, più di tutti, ha offerto la possibilità a coloro che vi operano di condividere, pubblicare e scambiare una gran numero di informazioni su scala globale.
Se, in un primo momento, esso era perciò considerato soltanto un grande archivio di dati e di servizi a disposizione degli utenti, successivamente si è compreso come questi ultimi possano avere, e di fatto hanno, anche un ruolo attivo in quanto produttori di contenuti personali (quali foto, video, blog).
Tutto ciò è stato facilitato anche dallo sviluppo di applicazioni sociali che hanno favorito, ad esempio, la creazione di vere e proprie comunità *on-line* nelle quali gli utenti possono trovare altri utenti con interessi simili, discutere di problemi comuni o semplicemente memorizzare o rendere accessibili risorse personali. Ciò che accade sui cosiddetti *social networks* (nominiamo i più noti, e cioè Facebook e Twitter) ne costituisce un modello.
Secondo alcuni, allora, è possibile asserire che Internet rappresenti nell'epoca contemporanea anche il maggior veicolo per l'esercizio di diritti come la libertà di espressione e di informazione e, allo stesso tempo, il diritto alla *privacy*. Scopriamone le ragioni.
La prima deriva direttamente dalle caratteristiche distintive della rete, vale a dire la sua rapidità (in termini di diffusione delle informazioni), la sua estensione su scala globale e la relativa anonimità degli utenti; insieme, questi elementi hanno contribuito allo sviluppo della capacità degli individui di disseminare informazioni in tempo reale e dar vita ad una spirale di perpetuo scambio di dati. Internet è diventato, dunque, un portale di accesso verso nuove conoscenze e una fonte preziosa per l'arricchimento personale e, pertanto, una risorsa rilevante grazie alla quale è possibile sviluppare la propria capacità di opinione ed espressione.
Lo stesso Relatore Speciale delle Nazioni Unite sulla promozione e protezione del diritto alla libertà di opinione e di espressione ha affermato che

> unlike any other medium the Internet facilitated the ability of individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an 'enabler' of other human rights, the Internet boosts economic, social and

> political development, and contributes to the progress of humankind as a whole[125].

D'altro canto, però, è necessario essere consapevoli anche della presenza delle numerose minacce e vulnerabilità presenti in rete, come egli ravvisa, raccomandando cautela agli utenti[126].
La seconda scaturisce dalla necessità di controllare, per quanto possibile, il flusso di dati che viaggia nelle reti informatiche e, più in generale, monitorare quanto avviene nel *cyber space*. La gran parte degli interrogativi che ci si pone riguarda soprattutto le garanzie offerte dalla rete circa la protezione di tutte quelle informazioni considerate sensibili che attraverso essa circolano.
Se da un lato, quindi, si ritiene un diritto il libero accesso alla rete, dall'altro ci si sta adoperando altresì per tutelare e proteggere i dati che vi fluiscono.
Il tema della protezione dei dati ha ormai assunto una certa rilevanza sia livello nazionale che internazionale, specialmente se teniamo in considerazione quanto detto nelle pagine precedenti: con sempre maggiore frequenza ad essere obiettivo di attacchi informatici sono tutti quegli enti in possesso di dati personali e, come abbiamo visto, solitamente gli *hackers* riescono a realizzare con relativa facilità ingenti furti di dati con conseguenze disastrose per istituzioni, organizzazioni, imprese e persone.
Nei prossimi paragrafi ci occuperemo di individuare i principali strumenti giuridici che contengono una disciplina in materia di diritti umani per capire se questi siano applicabili anche al contesto *cyber* e cercheremo di delineare un modello di strategia difensiva in risposta alla minaccia cibernetica che incrementi la capacità di prevenzione e risposta agli attacchi informatici e, contestualmente, il livello di protezione dei diritti fondamentali anche nello spazio cibernetico.
Il principio cardine consisterà, come vedremo, nel rafforzamento della capacità di gestione delle minacce mediante l'istituzione di efficaci meccanismi di allarme in caso di *cyber crimes* o *cyber attacks* in modo da garantire una maggiore protezione utilizzando altrettanta tecnologia e, contemporaneamente, nell'impegno a creare un *cyber* spazio non soltanto più sicuro ma anche aperto, accessibile e meno insidioso.

[125] LA RUE, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Rapporto del Consiglio dei Diritti Umani, 17esima sessione, 2011, reperibile *on-line*.
[126] *Ibidem.*

3.1 Il regime giuridico internazionale a tutela dei diritti umani

I diritti umani (o diritti dell'uomo) sono una branca del diritto e rappresentano l'insieme dei diritti inalienabili di cui ogni essere umano è titolare. Tra i diritti fondamentali dell'essere umano si possono ricordare, tra gli altri, il diritto alla libertà individuale, il diritto alla vita, il diritto all'autodeterminazione, il diritto a un giusto processo, il diritto alla libertà di opinione e di espressione, il diritto ad un'esistenza dignitosa, il diritto alla libertà religiosa con il conseguente diritto a cambiare la propria religione, oltre che, di recente tipizzazione normativa, il diritto alla protezione dei propri dati personali (o diritto alla *privacy*) e il diritto di voto.
Nell'ordinamento internazionale la tutela dei diritti umani è garantita sia da strumenti giuridicamente non vincolanti (la cui importanza non va sottovalutata, posto che spesso questi precedono la conclusione di trattati internazionali) sia da convenzioni internazionali che, una volta in vigore, vincolano però soltanto gli Stati che vi hanno preso parte e che le hanno ratificate. Queste possono avere carattere generale, in quanto elencano diritti di varia natura e contenuto, oppure carattere settoriale, a tutela soltanto di alcune categorie di soggetti (quali bambini, donne, migranti e via dicendo)[127]. Relativamente alla natura degli obblighi che da esse discendono, solo taluni diritti umani (come il diritto a non essere vittima di tortura) sono considerati assoluti e inderogabili; parimenti, tutti gli altri sono sottoponibili a restrizioni e limitazioni, purché siano rispettate diverse condizioni.
Enunciamo i principali riferimenti giuridici relativi alla tutela dei diritti umani.
Per quanto riguarda gli strumenti giuridicamente non vincolanti rileva, innanzitutto, la Dichiarazione universale dei diritti dell'uomo del 1948 approvata dalle Nazioni Unite e considerata il punto di partenza e il fondamento di un processo storico di approfondimento e di sviluppo dei diritti umani[128]. Di fatto, molte delle sue clausole risultano, oggi, giuridicamente vincolanti poiché trasformatesi in norme di diritto internazionale consuetudinario; essa, inoltre, ha rappresentato un modello e una fonte di ispirazione per la redazione di numerosi trattati internazionali in materi di diritti umani.
Altrettanto importanti sono gli strumenti giuridicamente non vincolanti elaborati dall'Organizzazione per la sicurezza e la cooperazione in Europa (l'Osce), che propone una concezione più ampia dei diritti umani disciplinando sia i rapporti tra l'individuo e le istituzioni sia i rapporti tra istituzioni stesse[129].

[127] PINESCHI (2012: 558 ss.).
[128] VILLANI (2015: 19).
[129] *Ibidem.*

Fra gli strumenti giuridicamente vincolanti, invece, è opportuno menzionare:

- la Convenzione per la prevenzione e la repressione del delitto di genocidio, elaborata dalle Nazioni Unite e adottata il 9 dicembre del 1948, mediante la quale si sancisce che il genocidio è un atto vietato dal diritto internazionale e che la sua perpetrazione può far scaturire tanto la responsabilità internazionale di uno Stato quanto la responsabilità penale di un individuo (perseguibile dalla Corte penale internazionale, istituita con il Trattato di Roma del 1998);
- la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, redatta e adottata nell'ambito del Consiglio d'Europa nel 1950;
- la Convenzione relativa allo statuto dei rifugiati, adottata nell'ambito delle Nazioni Unite nel 1951. Si tratta di un trattato multilaterale in cui è contenuta la definizione di 'rifugiato', dei diritti di cui godono i singoli individui che hanno ottenuto lo status di rifugiato e, infine, delle responsabilità e dei doveri delle nazioni che si trovano ad accogliere coloro che cercano rifugio;
- i due Patti delle Nazioni Unite del 1966 (il Patto sui diritti civili e politici e il Patto sui diritti economici, sociali e culturali);
- la Convenzione delle Nazioni Unite contro la tortura e altre pene o trattamenti crudeli, disumani o degradanti, approvata dall'Assemblea generale dell'ONU il 10 dicembre del 1984.

Relativamente al catalogo dei diritti dell'uomo contenuto in ognuno di questi atti è emersa una distinzione in diverse categorie o, come solitamente si sostiene, in 'generazioni' di diritti.
Questa classificazione, seppur convenzionale, è utile non soltanto per sistematizzare la materia ma anche per cogliere le origini, le istanze e le ideologie di cui tali diritti sono espressione[130].
Tradizionalmente sono state individuate quattro generazioni di diritti.
La prima di queste raccoglie i diritti civili e politici, aventi matrice essenzialmente occidentale e liberale, dei quali si sancisce il carattere innato in ogni essere umano: essi risultano, pertanto, riconoscibili in ogni tempo e in ogni luogo[131].
La seconda generazione ricomprende, invece, i diritti economici, sociali e culturali che per un verso, corrispondono alle istanze ed alle ideologie socialiste, per l'altro alla tradizione cristiana. Infatti, secondo la concezione socialista, l'uomo non è considerato un individuo astratto fornito di un complesso di diritti innati e immutabili ma un soggetto che vive in un dato momento storico con le sue esigenze e i suoi concreti bisogni. In tal senso, gli si riconoscono diritti quali il diritto al lavoro, il diritto di sciopero o il diritto all'assistenza sanitaria.

[130] *Ivi*, p. 20.
[131] *Ivi*, p. 21.

D'altra parte, in questa categoria di diritti ritroviamo anche la concezione cristiana tale per cui l'uomo scopre il suo valore all'interno della comunità in cui vive e nella quale egli si realizza, a cominciare dalla famiglia. Da qui, i diritti sociali.
La terza generazione di diritti nasce sulla base delle istanze dei Paesi del Terzo mondo, finalizzate a realizzare la liberalizzazione dei popoli dalla dominazione straniera e racchiude una serie di diritti che riguardano tanto l'individuo quanto i popoli. Tra questi ricordiamo, a titolo d'esempio, il diritto di autodeterminazione dei popoli, il diritto allo sviluppo o il diritto alla pace[132]. Con i diritti di terza generazione si compie un passo importante: si riconosce, infatti, che in una società ove sussistano condizioni di dominazione straniera, oppressione interna o sottosviluppo l'individuo non possa effettivamente esercitare tutti gli altri diritti di cui gode. Ne discende che i diritti dell'uomo vadano rivendicati, anzitutto, nei confronti del potere al quale ognuno è soggetto affinché, in primo luogo, sia esso ad eliminare le condizioni sfavorevoli alla loro fruibilità. Soltanto in un secondo momento la Comunità internazionale può essere chiamata/tenuta ad intervenire, nel rispetto di quanto stabilito dalle norme di diritto internazionale in materia.
Infine, abbiamo i diritti di quarta generazione che comprendono tutti quei diritti legati al rispetto della dignità umana e della sua integrità fisica e morale. Questi si sono sviluppati soprattutto in seguito ai recenti progressi scientifici in materia genetica. Fanno parte di tale categoria diritti quali il divieto di manipolazioni genetiche, il divieto di clonazione genetica o il divieto di pratiche eugenetiche.
Tutti questi diritti, e in particolare la tutela del patrimonio genetico dell'individuo, trovano la loro giustificazione nel rispetto della dignità umana e cioè nel dovere di tutelare il carattere unico e irripetibile di ogni essere umano[133]. In conclusione, l'affermazione di tali diritti ha l'obiettivo di chiarire che la ricerca scientifica è, e deve essere, strumentale al benessere della persona, trattata perciò come fine e non come mezzo poiché mai questa può essere assoggettata agli interessi della scienza e, in generale, della società.
Questa classificazione, seppur convenzionale, dimostra come il processo relativo alla tutela dei diritti umani sia in continua evoluzione ed espansione; nei prossimi paragrafi esamineremo le tappe più importanti di questo percorso che ha origine nel periodo successivo al 1945, anno in cui iniziano a proliferare i primi strumenti giuridici relativi alla tutela dei diritti dell'uomo in risposta agli orrori della II guerra mondiale.

La Carta delle Nazioni Unite

Abbiamo visto che tra i fini delle Nazioni Unite vi è il mantenimento della pace e della sicurezza internazionali. Questo lo si può realizzare non soltanto

[132] *Ibidem.*
[133] *Ivi*, p. 24.

garantendo l'assenza di situazioni di guerra ma anche mediante l'eliminazione delle cause che sono all'origine dei conflitti, solitamente consistenti nella mancanza di adeguate politiche di tutela dei diritti umani o nella presenza di cosiddette '*gross violations*' dei diritti umani.
La tutela dei diritti umani, pertanto, si presenta sia come un obiettivo da raggiungere e sia come uno strumento indispensabile per conseguire quello stesso scopo primario enunciato dalla Carta, consistente nel mantenimento della pace e della sicurezza internazionali.
Ad ogni modo, la Carta delle Nazioni Unite non contiene uno specifico elenco di diritti ma enuncia soltanto il c.d. 'principio di non discriminazione', diventato col tempo un diritto dotato di rilevanza autonoma, mediante il quale si sancisce l'impegno alla promozione della tutela dei diritti umani per tutti, senza distinzione di razza, di sesso, di lingua o di religione[134].
Secondo quanto stabilito, il compito di promuovere il rispetto dei diritti umani spetta sia all'Organizzazione in sé (e ai suoi organi) sia agli Stati che ne fanno parte. Ad ogni modo, è bene precisare che la Carta non contiene alcuna disposizione volta ad imporre agli Stati membri obblighi precisi in materia di tutela dei diritti umani né eventuali deroghe.
In seguito all'entrata in vigore della Carta sono stati elaborati numerosi strumenti giuridici vincolanti e non (fra i più importanti citiamo la Dichiarazione universale del 1948 e i Patti del 1966); inoltre, le Nazioni Unite hanno contribuito, e contribuiscono tutt'ora, alla promozione e al rispetto dei diritti umani mediante attività di monitoraggio e controllo, svolte dal Consiglio per i diritti umani, organo sussidiario istituito dall'Assemblea generale delle Nazioni Unite con la risoluzione del 15 marzo 2006, n. A/RES/60/251. Si tratta di un organo politico, composto da quarantasette rappresentanti degli Stati membri. Questi, sono eletti a scrutinio segreto dalla maggioranza dei membri dell'Assemblea generale anche in base al loro contributo verso attività di promozione e protezione dei diritti dell'uomo. A conferma di ciò vi sono anche due disposizioni restrittive circa la composizione del Consiglio: la prima stabilisce che nessuno Stato possa disporre di un seggio permanente né possa veder rieletto il proprio rappresentante per due mandati consecutivi; la seconda contempla la possibilità di sospensione per uno Stato membro che abbia commesso violazioni flagranti e sistematiche in materia di diritti umani (una decisione in tal senso deve, tuttavia, ottenere l'approvazione della maggioranza dei due terzi dei membri dell'Assemblea generale)[135].
Il Consiglio dei diritti umani è un organo politico dotato soltanto di poteri raccomandatori. Esso vigila sul rispetto dei diritti umani all'interno degli Stati membri dell'ONU mediante tre meccanismi di controllo.

[134] Carta delle Nazioni Unite del 1945.
[135] Tale sanzione è stata, ad esempio, adottata nel 2011 nei confronti della Libia su proposta del Consiglio dei diritti umani mediante la risoluzione del 25 febbraio 2011, n.S-15/1.

Il primo consiste nella '*universal periodical review*', vale a dire l'esame periodico (che avviene ogni quattro anni) dei rapporti predisposti dagli Stati stessi circa la situazione generale all'interno del proprio territorio e delle informazioni e dei dati forniti anche da altri organismi quali, ad esempio, l'Alto Commissariato delle Nazioni Unite, al fine di monitorare il livello di tutela dei diritti umani garantito dagli Stati membri.
Nell'ambito di tale attività, il Consiglio valuta la condotta degli Stati alla luce di alcuni strumenti giuridici rilevanti fra i quali la Carta delle Nazioni Unite, la Dichiarazione universale sui diritti umani e tutti i trattati internazionali in materia di cui uno Stato è parte; infine, esso deve far riferimento anche agli impegni assunti volontariamente dagli Stati al momento della sottoposizione della loro candidatura per l'elezione al Consiglio e agli obblighi ('applicabili') derivanti dal diritto internazionale umanitario.
Lo scopo principale di questa verifica non consiste nel comminare una sanzione ma nell'istaurare un dialogo e una cooperazione con tutti quegli Stati responsabili di violare gli obblighi derivanti dalla Carta al fine di migliorare la capacità di prevenzione o di pronta risposta a situazioni di emergenza in materia di *gross violations* dei diritti umani.
Il tutto si completa con un meccanismo di *follow up*, volto a monitorare l'attuazione delle raccomandazioni del Consiglio adottate al termine dell'esame periodico universale. A quest'ultimo, viene lasciata piena discrezionalità nel decidere se e quando sia necessario attivare tale meccanismo e cosa fare nell'eventualità in cui uno Stato persista nell'inadempienza degli obblighi internazionali e mostri scarso interesse a cooperare con il resto della Comunità internazionale.
Il secondo meccanismo è quello delle procedure speciali, nel quale entrano in gioco gruppi di esperti indipendenti designati dal Consiglio stesso che monitorano la condotta degli Stati membri delle Nazioni Unite in relazione soltanto a particolari categorie di diritti. Tali procedure consistono, per lo più, nella raccolta di informazioni (che avviene anche mediante visite *in loco*, previo consenso dello Stato interessato) e nella formulazione di raccomandazioni su particolari questioni o sulla situazione in determinati Paesi. Di nuovo, lo scopo non consiste nel sanzionare determinati comportamenti ma nella raccolta di informazioni fine con lo scopo di controllare quanto accade all'interno di uno Stato ed eventualmente prevenire l'aggravarsi della situazione.
Infine, abbiamo il meccanismo delle procedure di ricorso, che permette ad individui, gruppi di individui o organizzazioni non governative di segnalare al Consiglio violazioni gravi e sistematiche di qualsiasi diritto o libertà fondamentale. Quest'ultimo meccanismo, sebbene criticato per mancanza di trasparenza a causa della confidenzialità della procedura e poiché come misure finali prevede soltanto ulteriori forme di monitoraggio o meccanismi di assistenza, è molto importante poiché rappresenta ad oggi l'unica forma di ricorso internazionale a disposizione degli individui.

La Dichiarazione universale dei diritti dell'uomo

Attraverso l'adozione di tale documento da parte dell'Assemblea generale delle nazioni Unite, con risoluzione del 10 dicembre 1948, n. A/RES/217, per la prima volta gli Stati riconoscono in uno strumento giuridico a carattere universale l'importanza della tutela dei diritti dell'uomo in quanto tale e senza alcuna forma di discriminazione.
La maggior parte dei diritti in essa contenuti sono diritti civili e politici; ad ogni modo, essa contiene anche disposizioni relative alla tutela dei diritti economici, sociali e culturali.
A differenza di altri strumenti giuridici, in essa non si afferma esplicitamente l'inderogabilità di alcuno di questi diritti né sono state previste procedure di controllo sul rispetto del suo contenuto. Ciò nonostante, la maggior parte dei principi in essa contenuti hanno ormai assunto il carattere di norma consuetudinaria e, in quanto tali, sono vincolanti per tutti gli Stati della Comunità internazionale.
Tutto ciò è sostenuto anche dalla prassi internazionale, oggi ricca di trattati adottati in un momento successivo al 1948, di sentenze emesse da tribunali internazionali e nazionali, di atti adottati da diverse organizzazioni internazionali e di leggi nazionali che riprendono molti dei principi sanciti nel documento.
Infine, occorre sottolineare come alcuni principi, fra i quali il divieto di schiavitù (sancito dall'art. 4) o il divieto di tortura (art. 5) siano ritenuti tanto importanti da aver assunto persino natura di norma di diritto cogente e siano, cioè, inderogabili.
Nel documento, così come accade in altri strumenti giuridici in materia, si afferma, invece, la possibilità per gli Stati di introdurre limitazioni all'esercizio dei diritti ivi enunciati, purché sussistano le seguenti condizioni (sancite dall'art. 29):

1. tali limitazioni devono essere stabilite mediante legge;
2. il fine di tali limitazioni deve coincidere con l'assicurare il riconoscimento e il rispetto dei diritti di altri individui o per soddisfare le giuste esistenze della morale, dell'ordine pubblico e del benessere generale in una società democratica.

Come abbiamo già avuto modo di dire, la Dichiarazione universale non rappresenta uno strumento giuridicamente vincolante bensì una semplice dichiarazione di principi, espressione della volontà degli Stati di sottolineare l'importanza della promozione e del rispetto dei diritti dell'uomo. Dunque, essa non prevede l'istituzione di alcuna procedura di controllo sul rispetto dei diritti enunciati. Non di meno, proprio perché espressione di un impegno comune degli Stati membri delle Nazioni Unite, è stato chiaro fin da subito che qualsiasi comportamento in contrasto con quanto sancito da tale strumento avrebbe quantomeno rappresentato una violazione dell'art. 56

della Carta delle Nazioni Unite, che così stabilisce: "All Members pledge themselves to take joint and separate action in cooperation with the Organization". Inoltre, ricordiamo che, nell'ambito dell'esame periodico universale, il Consiglio dei diritti umani valuta la condotta degli Stati anche alla luce del contenuto della Dichiarazione.

Un' ultima considerazione da fare: quando essa venne adottata, le Nazioni Unite (e in particolare, il Consiglio dei diritti umani) stavano già lavorando ad un altro progetto che potesse portare, questa volta, alla conclusione di un trattato internazionale giuridicamente vincolante in materia di diritti umani. I negoziati, tuttavia, terminarono soltanto vent'anni dopo e si conclusero con l'adozione, nel dicembre del 1966, dei due Patti internazionali sui diritti civili, politici, economici, sociali e culturali e il relativo Protocollo facoltativo al Patto internazionale sui diritti civili e politici.
Entrambi rappresentano il primo esempio di strumenti giuridicamente vincolanti a carattere universale in materia di tutela dei diritti umani. Fra i due Patti non esiste una gerarchia: si tratta, infatti, di strumenti che coesistono e che si completano. Analizziamoli più nello specifico.

Il Patto internazionale sui diritti civili e politici

Diversamente dalla Dichiarazione universale, il Patto sui diritti civili e politici tutela tanto i diritti individuali quanto quelli collettivi, come i diritti riconosciuti alle minoranze[136].
Esso, inoltre, offre una tutela a volte più limitata circa alcune categorie di diritti rispetto a quella offerta dalla Dichiarazione.
Per quanto riguarda la natura degli obblighi previsti dal Patto a carico degli Stati questi sono di due tipi.
La prima tipologia prevede obblighi di astensione, vale a dire che gli Stati devono astenersi dall'adottare misure che possano limitare l'esercizio dei diritti contenuti nel Patto, se non nei casi previsti dal Patto stesso (che esamineremo a breve).
La seconda tipologia consiste in obblighi positivi (o obblighi di fare): ogni Stato deve adottare misure specifiche per permettere l'effettivo esercizio dei diritti sanciti dal Patto.
Per quanto riguarda eventuali restrizioni circa l'esercizio di taluni diritti, queste sono previste in caso di pericolo pubblico eccezionale, che minacci la vita della nazione, e purché lo stato di pericolo pubblico sia proclamato in un atto ufficiale e la parte interessata dia immediata comunicazione a tutti gli altri Stati parte della sua intenzione, presentando quali sono le disposizioni oggetto di possibile deroga e quali le ragioni di tale condotta. C'è da dire

[136] Patto sui diritti civili e politici, New York, 16 dicembre 1966, art. 27: "In those States in which ethnic, religious or linguistic minorities exist, persons belonging to such minorities shall not be denied the right, in community with the other members of their group, to enjoy their own culture, to profess and practise their own religion, or to use their own language".

che, però, taluni diritti sono categoricamente sottratti a questo regime di deroga.
Relativamente, invece, ai meccanismi di controllo posti a garanzia del rispetto delle norme contenute nel Patto, questi sono due.
Il primo implica un intervento diretto degli organi nazionali di ciascuno Stato parte (e nello specifico il suo apparato legislativo, esecutivo e giudiziario), i quali hanno la responsabilità principale di garantire l'effettivo rispetto delle norme contenute nel Patto.
Il secondo vede un intervento del Comitato dei diritti umani, un organo *ad hoc* istituito dal Patto stesso, composto da diciotto esperti di alta levatura morale e di riconosciuta competenza in materia di tutela dei diritti umani (eletti dagli Stati parte del Patto per un periodo di quattro anni, con possibilità di rielezione) che rappresenta, però, soltanto un mezzo di protezione secondaria o sussidiaria.
Tale organo vigila sulla condotta degli Stati mediante la valutazione dei rapporti periodici da questi redatti; inoltre, nei confronti degli Stati parte anche del Primo Protocollo facoltativo vi è la possibilità di ricezione da parte del Comitato di ricorsi statali e anche di ricorsi individuali.
Per quanto riguarda l'esame periodico dei rapporti, la procedura è specificata all'art. 40 del Patto che prescrive l'impegno degli State parte a sottoporre al Comitato dei diritti umani rapporti periodici sulle misure adottate per dare attuazione ai diritti ivi enunciati e sui progressi compiuti per assicurare il loro effettivo godimento. Fatta eccezione per il rapporto iniziale, presentato da tutti gli Stati entro un anno dall'entrata in vigore del Patto, tali rapporti devono essere sottoposti al vaglio del Comitato soltanto quando questo ne faccia richiesta. Ciò comporta, allora, la possibilità di condurre una più stretta vigilanza su alcuni Stati piuttosto che su altri.
L'art. 40 è piuttosto vago sui poteri che il Comitato può esercitare al termine dell'esame dei rapporti degli Stati: esso, solitamente, adotta per *consensus* delle osservazioni conclusive mediante le quali lo Stato può essere invitato a prestare più attenzione a determinate questioni e a fornire ulteriore riscontro entro un determinato periodo di tempo. Esse possono, altresì, contenere esplicite considerazioni sulla conformità di determinate situazioni rispetto ai diritti garantiti dal Patto e raccomandazioni circa la condotta che uno Stato dovrà tenere nel futuro. Se lo Stato non esegue quanto raccomandato, tale omissione sarà menzionata nel Rapporto annuale del Comitato all'Assemblea generale delle Nazioni Unite.
Dobbiamo considerare, tuttavia, il fatto che, sebbene la redazione dei rapporti periodici non sia una mera facoltà delle parti, il Comitato dei diritti umani non dispone di alcun potere coercitivo per imporre l'attuazione di tale obbligo.
Per quanto riguarda il secondo meccanismo di controllo e garanzia circa il rispetto delle norme contenute nel Patto, ai sensi dell'art. 41 dello stesso gli Stati possono proporre ricorsi al Comitato dei diritti umani qualora ritengano che uno o più Stati parte non abbiano adempiuto agli obblighi da esso derivanti. Tale procedura è, però, facoltativa nel senso che entrambi gli Stati

(quello che propone il ricorso e quello oggetto dello stesso) debbono aver preventivamente accettato la competenza del Comitato a ricevere tale ricorso. Ad oggi, nessun ricorso è stato ancora effettuato: nonostante il carattere *erga omnes* degli obblighi assunti prendendo parte al Patto, è evidente la reticenza degli Stati nel denunciare violazioni commesse dalle altre parti[137]. Ad ogni modo, è bene sapere che tale procedura termina con l'adozione di una soluzione amichevole, senza che sia prevista l'emanazione di alcun atto vincolante.
Infine, per quanto riguarda i ricorsi individuali in base al Primo Protocollo facoltativo al Patto si consente agli individui, che lamentino una presunta violazione dei propri diritti ad opera degli Stati parte, di proporre un ricorso al Comitato dei diritti umani.
Esistono, tuttavia, tre condizioni di ricevibilità che si esplicano in tre limiti:

1. *ratione personae,* in base al quale il ricorso deve essere presentato da un individuo, sottoposto alla giurisdizione di uno Stato parte, vittima di una violazione commessa da tale Stato.
2. *ratione materiae*, il quale impone che la violazione lamentata riguardi un diritto tutelato dal Patto.
3. *ratione temporis*, nei confronti dello Stato contro il quale viene proposto il ricorso che deve necessariamente entro sei mesi dalla trasmissione della comunicazione individuale da parte del Comitato inviare una risposta scritta contenente spiegazioni e/o dichiarazioni che chiariscano la situazione o che provvedano ad indicare le misure già adottate per rimediare.

Ricordiamo che, ad ogni modo, questa procedura è attivabile soltanto previo esaurimento dei mezzi di ricorso interni disponibili: questo, a tutela del principio di sovranità nazionale.
Quanto all'esame delle comunicazioni individuali, il Comitato decide sulla loro ricevibilità a porte chiuse mentre trasmette le sue osservazioni sia allo Stato oggetto del ricorso sia all'individuo autore dello stesso. Tali osservazioni non sono giuridicamente vincolanti, tuttavia le parti al Protocollo sono tenute ad un comportamento in linea con l'obbligo sottoscritto al momento dell'entrata in esso di cooperare in buona fede con il Comitato.
Non esistono neanche norme volte a monitorare l'adeguamento dello Stato alle osservazioni conclusive del Comitato; ciò nonostante, esso mediante un emendamento al suo Regolamento di procedura, può ora designare un relatore speciale che secondo l'art. 101 ha la facoltà di intraprendere "such contacts and take such action as appropriate for the due performance of the follow-up mandate" e di formulare raccomandazioni al Comitato circa eventuali ulteriori azioni da poter intraprendere.

[137] PINESCHI (2012: 576 ss.)

Infine, il Comitato dei diritti umani svolge un ruolo rilevante anche in merito all'interpretazione delle norme contenute nel Patto e nel Primo Protocollo facoltativo attraverso la redazione di commenti generali al fine di chiarire la natura, la portata e le modalità di applicazione delle stesse.

Il Patto sui diritti economici, sociali e culturali

Il primo aspetto da analizzare di questo documento riguarda la natura dei diritti ivi enunciati. Infatti, a differenza di quelli contenuti nel Patto sui diritti civili e politici, questi hanno natura essenzialmente programmatica: ogni Stato parte si impegna, di conseguenza, ad adottare tutte quelle misure necessarie ad assicurare 'progressivamente' la loro piena attuazione[138]. Ciò non significa che gli Stati possano rimandare l'effettiva implementazione delle norme del Patto ad un tempo indefinito né che la mancanza di risorse (economiche e non) possa giustificare il loro mancato rispetto, tuttavia non si tratta di norme ad efficacia diretta.
Per quanto riguarda, invece, la natura degli obblighi a carico degli Stati è possibile identificare tre categorie di obblighi:

1) gli obblighi negativi, che vietano agli Stati di adottare misure privanti l'effettivo godimento di determinati diritti o interferenti con il loro esercizio;
2) gli obblighi positivi, che consistono innanzitutto nell'adozione di tutte le misure necessarie a garantire l'accesso a determinate risorse o servizi e, in secondo luogo, nella garanzia di un buon funzionamento degli organi che vigilano e contrastino eventuali violazioni dei diritti contenuti nel documento;
3) gli obblighi di immediata attuazione.

Tale Patto non contiene, invece, alcuna clausola che permetta alle parti di derogare a parte dei diritti da esso sanciti in caso di emergenza. Viene riconosciuta, piuttosto, la possibilità di limitare la portata di qualsiasi diritto ivi contenuto purché sia assicurato il rispetto di quanto segue:

> […] the State may subject such rights only to such limitations as are determined by law only in so far as this may be compatible with the nature of these rights and solely for the purpose of promoting the general welfare in a democratic society.

Infine, per quanto riguarda i meccanismi di controllo, di nuovo rileva l'importanza fondamentale degli organi nazionali e delle garanzie offerte

[138] Patto sui diritti economici, sociali e culturali, New York, 16 dicembre 1966, art. 2 : "Each State Party to the present Covenant undertakes to take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures […]".

dagli ordinamenti interni di ciascuno Stato, mentre un ruolo sussidiario è affidato al Comitato dei diritti economici, sociali e culturali, istituito nel 1985, che svolge quell'attività di monitoraggio che, secondo quanto stabilito dal Patto, doveva essere svolta da un organo politico: l'ECOSOC.
Il Comitato è composto da diciotto individui (di comprovata competenza in materia di tutela dei diritti umani), eletti dall'ECOSOC per un periodo di quattro anni, rieleggibili; questi devono, prima di assumere l'incarico, dichiarare solennemente di esercitare le proprie funzioni in modo imparziale.
Come già esaminato nel caso del Patto sui diritti civili e politici, anche qui si contemplano tre meccanismi di vigilanza e controllo:

1. l'analisi dei rapporti periodici degli Stati, mediante la quale il Comitato vigila sulle misure adottate dagli Stati per dare attuazione alle norme previste dal Patto. Contrariamente a quanto fa il Comitato dei diritti umani, però, esso non trasmette direttamente le proprie osservazioni agli Stati ma all'ECOSOC. Anche esso ha adottato procedure di monitoraggio sul comportamento degli Stati in seguito alla valutazione dei rapporti periodici o in risposta all'inadempienza di uno Stato che ritardi a presentare i propri rapporti periodici. Inoltre, a partire dal 1991, il rapporto di uno Stato può essere esaminato in assenza di un suo rappresentante, qualora la sua discussione venga ripetutamente rinviata per colpa dello Stato[139].
2. le comunicazioni inter-statali (previste insieme a quelle individuali dal Protocollo facoltativo al Patto del 2008, non ancora entrato in vigore), la cui possibilità di presentazione è subordinata a una dichiarazione facoltativa dello Stato interessato e opera soltanto a condizioni di reciprocità[140].
3. le comunicazioni individuali, le cui condizioni di ricevibilità sono sostanzialmente identiche a quelle previste dal Protocollo facoltativo al Patto sui diritti civili e politici. Le uniche novità consistono nel fatto che per quanto riguarda i limiti *ratione personae*, le comunicazioni possono essere introdotte sia da individui sia da gruppi di individui, purché la vittima o le vittime esprimano un loro consenso preventivo (questo vale a meno che gli autori della comunicazione non possano fornire giustificazioni per agire senza il rispetto di tale requisito). Tale estensione del diritto in esame anche a gruppi di individui o a soggetti che agiscono per conto di presunte vittime costituisce una novità significativa sia sul piano formale, sia sul piano sostanziale, considerando che alcuni diritti tutelati dal Patto si caratterizzano, per loro natura, di fatto non solo come diritti individuali, ma anche come diritti collettivi[141].

[139] PINESCHI (2012: 578 ss.)
[140] Protocollo facoltativo al Patto sui diritti economici, sociali e culturali del 2008, art. 10.
[141] *Ibidem*.

> Per quanto riguarda i limiti *ratione materiae*, le comunicazioni individuali possono avere per oggetto la violazione di qualsiasi diritto enunciato nel Patto sui diritti economici e sociali. Questa soluzione è tutt'altro che scontata, poiché nel corso dei negoziati alcuni Stati si erano opposti a un simile approccio globale[142].

Ad essi, dobbiamo aggiungere anche la procedura d'inchiesta, che può essere avviata dal Comitato, previa dichiarazione di accettazione, meramente facoltativa e revocabile in qualsiasi momento, dello Stato interessato, qualora esso riceva informazioni attendibili sulla presunta violazione grave o sistematica di qualunque diritto enunciato dal Patto ad opera di uno Stato parte. Tale procedura è disciplinata direttamente dal Protocollo del 2008. L'aspetto chiave, che forse la rende meno efficace, presuppone la costante cooperazione dello Stato interessato; inoltre, la procedura è confidenziale e lascia ampia discrezionalità al Comitato circa il meccanismo di *follow-up*.
Da ultimo, anche il Comitato dei diritti economici, sociali e culturali svolge una funzione interpretativa mediante la redazione di commenti generali volti a chiarire il contenuto del Patto e a precisare alcuni degli obblighi procedurali previsti, a carico degli Stati parte.

[142] PINESCHI (2012: 579).

3.2 La tutela dei diritti umani a livello regionale: il sistema europeo

Numerosi strumenti a tutela dei diritti umani sono sorti anche nell'ambito di organizzazioni regionali; in tale contesto, in Europa si è provveduto alla costruzione di un complesso meccanismo di protezione dei diritti umani che merita di essere analizzato.
Il principale punto di riferimento è costituito dal Consiglio d'Europa, organizzazione fondata il 5 maggio 1949 con il Trattato di Londra (che conta oggi 47 stati membri) che si occupa della promozione della democrazia, dei diritti umani e dell'identità culturale europea.
Il primo e più importante documento elaborato nell'ambito del Consiglio d'Europa è la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, adottata a Roma nel 1950.
Essa è stata elaborata sulla base di quanto è stato sancito dalla Dichiarazione universale e, tuttavia, da questa si discosta laddove si concentra, per lo più, sulla salvaguardia dei diritti civili e politici. La tutela dei diritti economici, sociali e culturali in ambito europeo è, infatti, affidata ad un altro strumento: la Carta sociale europea (adottata a Torino il 18 ottobre 1961).
Per quanto riguarda gli obblighi a carico degli Stati tale convenzione dà luogo sia ad obblighi di astensione sia ad obblighi positivi.
L'ambito di applicazione della stessa è, invece, sancito all'art. 1 che afferma: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention"[143]. Da notare l'impiego del termine giurisdizione, che sta ad indicare tanto il territorio di uno Stato quanto il suo mare territoriale e lo spazio aereo sovrastante; inoltre, ricordiamo che essa contempla, in un certo senso, anche forme di applicazione extra-territoriale, come suggerito dalla giurisprudenza della Corte europea dei diritti dell'uomo. Quest'ultima ha imposto, infatti, l'obbligo per gli Stati parte di tutelare gli individui e assicurare il rispetto dei diritti sanciti dalla Convenzione di cui essi godono anche nel caso in cui, a seguito di fenomeni come l'espulsione, questi sarebbero violati da Stati non parte della Convenzione stessa. Ciò significa che, prima di procedere all'espulsione di un individuo, lo Stato parte deve accertarsi che nello Stato di destinazione egli non veda violati i diritti sanciti nel documento poiché, qualora ciò avvenisse, esso sarebbe considerato ugualmente responsabile di tale violazione[144].
Al pari di altri strumenti giuridici, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali prevede comunque forme di limitazione che consentono agli Stati parte di restringere l'esercizio di alcuni diritti di fronte ad esigenze di carattere pubblico o al fine

[143] Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, Roma, 4 novembre 1950.
[144] Sentenza della Corte europea dei diritti dell'uomo del 15 novembre 1996, n. 14038, *Soering c. Regno Unito*.

di tutelare i diritti di altri individui. Anche in questo caso, però, devono essere rispettate talune condizioni.
Nello specifico, si prevede che:

a) tali limitazioni debbano essere previste per legge;
b) tali limitazioni debbano perseguire uno scopo consentito, di volta in volta, dalla Convenzione stessa (quali ad esempio la tutela dell'ordine pubblico o la sicurezza nazionale);
c) debbano essere necessarie in una società democratica al fine di raggiungere tale scopo.

La Convenzione contiene poi una norma che consente di derogare ai diritti in essa sanciti, in particolare in caso di guerra o altra emergenza che minacci la vita della nazione. A tal proposito l'art. 15 della Convenzione afferma che:

> in time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.

Ad ogni modo, anche l'applicazione dell'art. 15 è subordinata al rispetto di alcune condizioni: infatti, le misure adottate devono rispettare i requisiti di necessità e proporzionalità. Inoltre, le deroghe non devono essere incompatibili con altri obblighi internazionali.
Al comma 2 dello stesso si afferma, inoltre, che il limite dello stato di emergenza non possa essere invocato per alcuni diritti (vale a dire il diritto alla vita che, pur essendo annoverato fra i diritti assoluti, è comunque soggetto, in tempo di conflitto armato, alle limitazioni derivanti dai 'legittimi atti di guerra'. Seguono il divieto di tortura, il divieto di schiavitù e lavori forzati e il principio *nulla poena sine lege*).
Viene, altresì, stabilito che lo Stato parte che si avvalga del diritto di deroga è tenuto al rispetto di un obbligo procedurale, consistente nel fornire informazioni al Segretario generale del Consiglio d'Europa circa le misure adottate e le ragioni che le hanno ispirate, nonché la data in cui tali misure hanno cessato di essere in vigore, come sancito al comma 3 dell'art. 15, in cui si afferma quanto segue:

> any High Contracting Party availing itself of this right of derogation shall keep the Secretary General of the Council of Europe fully informed of the measures which it has taken and the reasons therefor. It shall also inform the Secretary General of the Council of Europe when such measures have ceased to operate and the provisions of the Convention are again being fully executed.

Per quanto riguarda i meccanismi di garanzia e controllo, il sistema europeo è uno dei più complessi.

Ad espressione della volontà di assicurare la presenza di un sistema efficace è stato istituito un vero e proprio organo giudiziario che ha assunto carattere permanente nel 1998 (con l'entrata in vigore del Protocollo n. 11): la Corte europea dei diritti umani, la quale agisce in osservanza del principio di sussidiarietà rispetto all'intervento degli organi interni di uno Stato.
La Corte è composta da tanti giudici (il cui mandato dura nove anni) quanti sono gli Stati parte; essi sono eletti dall'Assemblea parlamentare del Consiglio d'Europa a maggioranza dei voti espressi, sulla base di una lista di tre candidati presentati da ciascuno Stato parte. Nessun giudice può essere rieletto scaduto il proprio mandato.
La composizione della Corte è variabile. Per la trattazione dei ricorsi, la Corte siede quale giudice unico, in comitati di tre giudici, in Camere di sette giudici e in una Grande Camera di diciassette giudici.
Tra le novità che l'istituzione di tale organo ha prodotto troviamo il riconoscimento agli individui di un vero e proprio diritto di azione davanti alla Corte, la cui giurisdizione sui ricorsi individuali deriva direttamente dalla Convenzione stessa[145].
Quanto all'esame di tali ricorsi, il Protocollo n. 14 ha introdotto significativi emendamenti volti ad accelerare e semplificare le procedure.
Oggi, si prevede l'intervento di un giudice unico (non avente la stessa nazionalità dello Stato convenuto) che può dichiarare la loro non ricevibilità oppure la loro cancellazione dal ruolo, qualora l'inammissibilità sia manifesta (secondo i criteri stabiliti dall'art. 35[146]).
Qualora sorgano dubbi, il ricorso viene trasmesso ad un comitato di tre giudici che può, all'unanimità, dichiarare il ricorso inammissibile (in tal caso, la decisione è definitiva) oppure, in un'unica decisione, dichiarare la sua ammissibilità e pronunciarsi sul merito, se la questione sottoposta è stata già oggetto di una giurisprudenza consolidata della Corte.

---

[145] PINESCHI (2012: 572 ss.).
[146] Convenzione europea dei diritti dell'uomo del 1950, art. 35:
"The Court may only deal with the matter after all domestic remedies have been exhausted, according to the generally recognised rules of international law, and within a period of six months from the date on which the final decision was taken.
The Court shall not deal with any application submitted under Article 34 that
(a) is anonymous; or
(b) is substantially the same as a matter that has already been examined by the Court or has already been submitted to another procedure of international investigation or settlement and contains no relevant new information.
The Court shall declare inadmissible any individual application submitted under Article 34 if it considers that:
(a) the application is incompatible with the provisions of the Convention or the Protocols thereto, manifestly ill-founded, or an abuse of the right of individual application; or
(b) the applicant has not suffered a significant disadvantage, unless respect for human rights as defined in the Convention and the Protocols thereto requires an examination of the application on the merits and provided that no case may be rejected on this ground which has not been duly considered by a domestic tribunal.
The Court shall reject any application which it considers inadmissible under this Article. It may do so at any stage of the proceedings".

Accanto questo tipo di ricorsi sussistono i ricorsi statali, che possono essere promossi da tutti gli Stati parte, i quali possono adire la Corte qualora uno di questi violi la Convenzione. A differenza di altri trattati a tutela dei diritti umani, l'accettazione della giurisdizione della Corte non avviene attraverso una dichiarazione separata, ma è implicita nella partecipazione alla Convenzione europea. Nei casi in cui la Corte abbia giurisdizione (*ratione personae, temporis, materiae* e *loci*), le sole condizioni di ricevibilità consistono nel soddisfacimento del requisito del previo esaurimento dei ricorsi interni e nel rispetto della regola secondo la quale il ricorso deve essere introdotto entro sei mesi dalla decisione interna definitiva (come si afferma al comma 1 dell'art. 35 della Convenzione).
Sulla ricevibilità e sul merito dei ricorsi proposti dagli Stati si pronuncia una Camera (art. 29, comma 2), al cui interno siede di diritto il giudice della nazionalità dello Stato parte alla controversia. Lo stesso requisito è previsto qualora sul caso si pronunci la Grande Camera (art. 26, comma 4).
Al termine del procedimento la Corte dichiara l'eventuale violazione della Convenzione europea e dei suoi Protocolli e può accordare alla parte lesa, se lo ritiene necessario, un'equa soddisfazione (consistente, in genere, nel pagamento di un indennizzo) laddove l'ordinamento nazionale non consenta la rimozione delle conseguenze della violazione (come si afferma nell'art. 41 della Convenzione stessa).
Le sentenze della Grande Camera sono definitive.
Data l'essenzialità della piena e rapida esecuzione delle sentenze della Corte al fine di rendere credibile il suo ruolo circa l'attuazione delle pronunce della stessa, nel Protocollo n. 14 sono state attribuite nuove competenze al Comitato dei ministri (organo decisionale del Consiglio d'Europa). Questo, è chiamato a vegliare sull'esecuzione delle sentenze e sul rispetto dei termini di regolamento contenuti nelle decisioni della Corte che hanno cancellato una causa dal ruolo in seguito a composizione amichevole.
Per quanto concerne l'attuazione delle sentenze definitive, l'art. 46, contempla due nuove procedure:

- la prima comporta che, qualora il Comitato dei ministri ritenga che l'esecuzione di una sentenza definitiva sia ostacolata dal disaccordo tra le parti in merito alla sua interpretazione, esso possa adire la Corte, invitandola a pronunciarsi sulla questione. La norma non pone limiti temporali all'azione del Comitato dei ministri; al fine, però, di evitare un ulteriore sovraccarico di lavoro della Corte, la decisione del Comitato deve essere assunta a maggioranza qualificata.
- la seconda contempla la possibilità per il Comitato dei ministri di adire la Corte qualora esso ritenga che uno Stato parte non si sia conformato ad una sentenza definitiva emessa nei suoi confronti. Se la Corte accerta la violazione dell'obbligo di conformazione, il Comitato dei ministri è autorizzato ad adottare le misure che ritiene necessarie.

Nel tempo, il ruolo della Corte europea dei diritti dell'uomo è diventato fondamentale per almeno due ragioni.
La prima riconosce alla Corte un ruolo particolare circa l'ampliamento della portata delle garanzie della Convenzione, avvenuto mediante l'affermazione del 'principio di effettività' che ha prodotto un'estensione dei poteri di controllo della Corte stessa anche in relazione a diritti non esplicitamente previsti nel documento.
La seconda ragione guarda alla capacità della Corte di prestare attenzione all'importanza strumentale degli obblighi procedurali per una tutela effettiva degli obblighi sostanziali e di assicurare un'uniformità circa l'interpretazione della Convenzione grazie ai suoi pareri o alle sue decisioni.

3.3 Cyber security e tutela dei diritti umani

In seguito a questa breve analisi dei principali strumenti giuridici in materia di diritti umani a livello internazionale e regionale, proseguiamo con una panoramica della disciplina a livello internazionale, regionale e nazionale relativa alla protezione di due diritti che, in particolar modo, rilevano all'interno del contesto *cyber*: la libertà di espressione e il diritto alla *privacy*.

Libertà di espressione

Utilizzando il linguaggio dei diritti umani, si sente spesso parlare di '*Internet freedom*', un concetto che fa riferimento al diritto di accesso ad Internet come mezzo per e al fine di connettere gli individui a livello globale.
La questione della libertà in rete non è, però, di semplice discussione; esistono, infatti, Paesi ove ancora questa non è garantita: pensiamo alla Cina[147] o all'Iran[148], che hanno adottato politiche di censura nei confronti di diversi notiziari *on-line* o *social network*. Questo accade principalmente perché Internet è oggi un mezzo di comunicazione dotato di forte influenza.
Per capire meglio le ragioni che si nascondono dietro queste misure politiche basti pensare ai recenti eventi che hanno coinvolto numerosi Paesi del Nord Africa e del Medio oriente, identificati come Primavere arabe.
Secondo alcuni esperti, fra i quali Philip Howard e Muzammil Hussain, sebbene il dissenso e il malcontento fossero presenti nelle popolazioni dei Paesi coinvolti in questo processo di rivoluzione già prima della diffusione di Internet, il poter comunicare nel mondo virtuale ha permesso la condivisione e lo scambio di opinioni e di informazioni con altre persone che nutrivano gli stessi sentimenti e ha, altresì, permesso la mobilitazione di massa mediante l'organizzazione di eventi e proteste in luoghi specifici[149].
In più, attraverso la diffusione di dati e di informazioni riguardanti i loro Paesi e quelli occidentali, Internet ha rivelato alle popolazioni locali rispettivamente la corruzione dei propri regimi politici e la possibilità di ottenere condizioni di vita differenti.
In conclusione, i *social media* hanno rappresentato un luogo virtuale in cui poter esprimere sentimenti quali insoddisfazione e sostegno reciproco; un luogo che da virtuale è diventato reale e che ha certamente favorito la realizzazione di proteste di massa contro i regimi autoritari presenti nella regione.
Contemporaneamente, Internet ha mostrato a tutto il resto della comunità internazionale cosa stava accadendo, giocando un ruolo fondamentale nello

[147] EADS, *China's Newest Export: Internet Censorship*, in *USNews*, 30 gennaio 2014, reperibile *on-line*.
[148] LEE, *Here's how Iran censors the Internet*, in *The Washington Post*, 15 agosto 2013, reperibile *on-line*.
[149] BECK, HUSEN (2013: 2 ss.).

scacchiere internazionale: di fatto, si è registrato un effetto domino nei Paesi vicini e uno schieramento delle altre potenze con l'una o con l'altra parte.
Le Primavere Arabe hanno mostrato nuovamente al mondo, in chiave diversa, la potenza del *cyber space:* questa è la principale ragione per cui un regime politico autoritario, se vuole sopravvivere, deve ora anche cercare di controllare, ciò che accade in rete, al fine di impedire alla popolazione a sé assoggettata il confronto con realtà diverse o con persone altrettanto insoddisfatte insieme alle quali si potrebbero organizzare movimenti di protesta o 'rivoluzioni di massa'.
Una censura in Internet può avvenire, tuttavia, anche per altre ragioni: ad esempio, a seguito di politiche di *cyber security* o in generale di sicurezza nazionale molto restrittive a fronte dell'idea che un maggior controllo possa garantire contestualmente una maggiore sicurezza. Come vedremo questo è vero solo in parte: è quanto mai necessario, infatti, attuare politiche di sicurezza che comunque non violino i diritti fondamentali dell'uomo, i quali vanno rispettati al di là del contesto reale o virtuale in cui ci troviamo ad operare.
Anche in seguito ad attacchi informatici può verificarsi una violazione dei diritti umani: pensiamo agli attacchi DDoS (che escludono l'accesso a siti o pagine di Internet) oppure ad attacchi come quello che ha colpito la JP Morgan Chase & Co, finalizzato al furto dei dati personali dei clienti della società americana.
Concentrandoci per il momento sul diritto alla libertà di espressione, esploriamo le modalità mediante le quali è possibile bloccare l'accesso ai contenuti presenti in rete, sia che si tratti di un sito Internet sia che si tratti di una sola specifica pagina.
Esistono, infatti, differenti tecniche aventi ognuna un certo livello di efficacia e di effetti.
Una prima strada che si può intraprendere è quella che utilizza l'indirizzo IP (*Internet Protocol*, ossia l'insieme dei numeri che identifica univocamente un dispositivo connesso ad una rete informatica)[150]; esso garantisce il corretto traffico di dati nella rete secondo vie sicure che permettono di arrivare a destinazione e cioè al sito o alla pagina Internet alla quale un utente vuole accedere. Un'eventuale misura di blocco impedisce che ciò avvenga, indirizzando di fatto il traffico di dati verso una via non esistente e impedendo, dunque, l'accesso ad una pagina o un sito *on-line*.
Questo tipo di misura ha però, se così possiamo dire, degli effetti collaterali: è possibile che, attuandola, anche il contenuto legittimo di altri siti o pagine venga oscurato, con la conseguente estensione del divieto di accesso a contenuti che non sarebbero dovuti essere da questo interessati.
Vediamo ora il secondo metodo. Esso impiega il c.d. URL (e cioè la sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet)[151] e, similmente a quanto accade mediante l'utilizzo del primo

[150] KULESZA, BALLESTE (2016: 87 ss.).
[151] *Ibidem.*

metodo, mediante tale tecnica si impedisce la visualizzazione di intere pagine o contenuti di queste. Anche in questo caso esistono dei rischi: il principale è quello relativo alla produzione di un *'overblocking',* che può generarsi da un erronea identificazione dell'URL provocando l'arresto dell'intera piattaforma Internet. Questo è ciò che è accaduto nel caso *Yildirim c. Turchia,* quando il governo turco decise di interrompere l'accesso ad un sito Internet che insultava la memoria del fondatore della Repubblica di Turchia, Mustafà Kemal, ma causò invece il blocco dell'intera piattaforma di Google[152].

Una terza procedura consiste nel bloccare direttamente il *domain name system* (DNS), che non è altro se non un grande archivio gerarchico e distribuito in cui ci sono le corrispondenze tra domini e indirizzi IP (di modo che per trovare un sito non si debba memorizzare questi ultimi ma è sufficiente conoscere, per l'appunto, il dominio di un sito[153]). Esso, in pratica, memorizza dove il contenuto di un sito è collocato all'interno della rete informatica. Per bloccare l'accesso a quest'ultimo si 'riscrive' la risposta che il DNS darà in seguito alla richiesta da parte di un utente di essere indirizzato verso un particolare sito o una particolare pagina di modo che il sistema risponda con un messaggio relativo all'inesistenza di quel particolare contenuto. In alternativa, il sistema potrebbe indirizzare l'utente verso altri contenuti che includano, piuttosto, un messaggio di allerta. Il risultato a cui si perviene è il medesimo: si impedisce il libero accesso a siti o pagine Internet.

Alcuni esperti sostengono che questo tipo di misura colpisca un elemento fondamentale di Internet, senza il quale esso non esisterebbe, e che nei fatti all'utente venga detta una bugia. Essi, perciò, supportano l'idea per cui tale tecnica non dovrebbe essere utilizzata[154]. Peraltro, occorre considerare quanto si afferma all'art. 10 della Convenzione europea dei diritti dell'uomo e cioè che la libertà di espressione deve essere garantita senza che vi sia ingerenza da parte delle autorità pubbliche[155]. Questo, anche in nome del

---

[152] *Ibidem.*

[153] Ad esempio, per quanto riguarda l'indirizzo www.fastweb.it ciò che occorre ricordare è il dominio (e cioè fastweb.it) ma ad esso corrisponde certamente un indirizzo IP, certamente molto più complicato da ricordare (in questo caso esso è 62.101.76.232). L'utilizzo dei domini, piuttosto che l'utilizzo degli indirizzi IP, facilità gli utenti nel momento in cui occorre loro cercare un sito specifico.

[154] *Ibidem.*

[155] Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, Roma, 3 settembre 1953, art. 10: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of

concetto di 'trasparenza' della gestione della *res publica*, da realizzare sia mettendo a disposizione dei cittadini le informazioni sia facendole circolare liberamente e rimuovendo tutti i possibili ostacoli all'effettivo accesso ad esse da parte dei cittadini.
Il diritto alla libertà di espressione è contenuto in diversi strumenti giuridici, che in parte abbiamo già citato, ed è del tutto applicabile al contesto *cyber*.
Esaminiamo, innanzitutto, le norme internazionali a riguardo.
Il diritto alla libertà di espressione trova la sua prima proclamazione alle Nazioni Unite nell'ambito della Dichiarazione universale dei diritti dell'uomo agli articoli 12, 19 e 27.
Il primo di questi articoli chiarisce immediatamente che la tutela della libertà di espressione debba essere garantita senza che vi sia ingerenza da parte delle autorità pubbliche.
Esso recita quanto segue:

> no one shall be subjected to arbitrary interference with his *privacy*, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks[156].

L'art. 19 è, invece, utile per capire perché possiamo ritenere applicabili tali norme internazionali anche ad Internet. Esso, infatti, parla di diritto a 'cercare', 'ricevere' e 'diffondere' informazioni[157]: questo è esattamente ciò che accade in rete; come già detto, mediante Internet, gli utenti possono ricercare, ricevere e, a loro volta, pubblicare informazioni realizzandone quindi la diffusione.
Tale articolo risulta ulteriormente rafforzato da quanto afferma l'art. 27 della Dichiarazione, il quale stabilisce il diritto di ogni individuo a partecipare liberamente alla vita culturale della comunità, a godere delle manifestazioni artistiche e dei benefici connessi con lo sviluppo scientifico. Dato che alla base di Internet vi è lo anche scambio di informazioni di natura culturale e scientifica, l'art. 27 è riferibile anche al contesto delle *cyber operations*, nonostante sia stato formulato in epoca diversa.
Abbiamo visto che i principi enunciati nella Dichiarazione universale sono stati successivamente ripresi e ulteriormente sviluppati mediante altri strumenti giuridici, fra i quali innanzitutto i Patti nel 1966.
L'art. 19 del Patto internazionale sui diritti civili e politici riprende quasi letteralmente l'art. 19 della Dichiarazione; diversamente da questo, tuttavia, il Patto si esprime in maniera più specifica affermando che il diritto alla libertà di espressione include anche la libertà di

---

information received in confidence, or for maintaining the authority and impartiality of the judiciary".
[156] Dichiarazione universale dei diritti dell'uomo del 1948.
[157] Dichiarazione universale dei diritti dell'uomo del 1948, art. 19: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers".

> seek, receive and import information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice[158].

Dunque, si fa riferimento innanzitutto alla portata di tale libertà, che deve essere garantita a prescindere dai confini territoriali di uno Stato e a prescindere dalle modalità o dagli strumenti attraverso i quali avviene lo scambio di informazioni.
Il Patto riprende anche il concetto, di cui all'art. 12 della Dichiarazione, relativo al divieto di interferenze arbitrarie o illegittime da parte di un'autorità pubblica nella sfera privata degli individui.
Successivamente, il Patto provvede a delineare la portata delle limitazioni che possono essere imposte alla libertà di espressione. Si stabilisce, innanzitutto, che eventuali restrizioni debbano essere espressamente stabilite per legge; inoltre, esse devono essere indispensabili per:

a) assicurare il rispetto dei diritti o della reputazione altrui;
b) la protezione della sicurezza nazionale, l'ordine pubblico, la salute o la morale pubbliche.

Appare quanto mai doveroso per gli Stati, dunque, dimostrare che una limitazione ai diritti contenuti nel Patto (fra cui per l'appunto il diritto alla libertà di espressione) sia necessaria e far sì che le norme che impongono tali restrizioni siano aperte, specifiche e chiare[159].

A livello regionale rileva, soprattutto, l'art. 10 della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali nonché la sua interpretazione da parte della Corte europea dei diritti umani.
Esso sancisce che

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[158] Patto sui diritti civili e politici, New York, 16 dicembre 1966.
[159] SORDINI (2013: 12).

In altre parole, accanto alla tradizionale interpretazione del diritto alla libertà di espressione quale sfera di autonomia privata protetta da ingerenze esterne si fa anche riferimento ad una dimensione pubblica di tale libertà intesa come libertà di ricevere o di comunicare informazioni e idee.
I confini della libertà di espressione sono stati, inoltre, ulteriormente ampliati dalla giurisprudenza della Corte europea dei diritti dell'uomo che ha provveduto ad integrare il semplice dettato normativo.
Essa ha, innanzitutto, specificato che rientra all'interno della sfera di garanzia di cui all'art. 10 della Convenzione ogni mezzo di comunicazione e diffusione delle notizie[160]. Inoltre, occorre considerare che il diritto alla libertà di espressione include anche tutte quelle comunicazioni che travalicano i confini di uno stato; pertanto, possiamo ritenere applicabile anche tale norma al contesto *cyber*, caratterizzato proprio dalla interconnessione a livello globale delle sue reti e, dunque, dello scambio di informazioni al di là dei confini territoriali di uno Stato.
Proseguendo nella lettura dell'art. 10 arriviamo al secondo comma. Questo, individua le ragioni e i casi per cui possono essere posti eventuali limiti a tale libertà.
A lasciare perplessi molti esperti è la particolarità con cui si elencano i numerosi casi in cui uno Stato nazionale possa imporre limitazioni all'esercizio della libertà di espressione e dunque, almeno in parte, venir meno alla tutela garantita dal precedente paragrafo.
Nel dettaglio, si tratta dei casi in cui misure restrittive sono necessarie in una società democratica per:

a) tutelare la sicurezza nazionale;
b) tutelare l'integrità territoriale;
c) tutelare l'ordine pubblico;
d) prevenire i reati;
e) proteggere la salute;
f) proteggere la morale;
g) proteggere la reputazione o i diritti altrui;
h) impedire la divulgazione di informazioni confidenziali;
i) garantire l'autorità e l'imparzialità del potere giudiziario.

Nonostante la presenza di quest'elenco, occorre sottolineare come alcuni termini impiegati siano troppo generici e indefinibili.
Risulta fondamentale, allora, l'interpretazione della Corte europea dei diritti dell'uomo, la quale ha affermato che "any restriction imposed on access to content necessarily interferes with the right to receive and impart information"[161], ogni qualvolta siano bloccati dei siti si deve anche

[160] Sentenza della Corte europea dei diritti dell'uomo del 10 ottobre 2013, *Delfi AS c. Estonia*, ricorso n. 64569/09.
[161] Sentenza della Corte europea dei diritti umani del 19 febbraio 2013, 40397/12, *Neij and Sunde Kolmisoppi c. Svezia*.

comprendere se tali azioni siano compatibili con una sufficiente tutela della libertà di espressione, al fine di valutarne la legittimità.
A tal proposito, occorre allora capire se sussistono delle circostanze che giustificherebbero tali misure o se, al contrario, allo scopo di garantire la libertà di espressione si debba sempre considerare illecito bloccare l'accesso ad Internet o a parte dei suoi contenuti.
In materia, la Corte europea ha fornito un'utile interpretazione. Essa ha, innanzitutto, sancito che

> blocking access to the Internet, or parts of the Internet, for whole populations or segments of the public can never be justified, including in the interests of justice, public order or national security.

Nel caso *Yildirim c. Turchia*, ad esempio, la Corte europea ha esplicitamente sostenuto che impedire l'accesso al sito ad una larga parte di popolazione aveva rappresentato un'interferenza del governo turco e una violazione dell'art. 10 della Convenzione.
Essa, poi, ha tenuto a specificare nuovamente quanto si afferma nella stessa Convenzione in relazione alle misure restrittive, vale a dire che, se prese, queste devono essere previste per legge[162] e devono costituire misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione di reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui[163]. Questo, dunque, implica che uno Stato che voglia perseguire una politica caratterizzata da misure restrittive riguardanti il libero accesso ai contenuti di Internet deve fornire una giustificazione[164] della sua condotta sufficientemente valida da scagionarlo da qualunque accusa di abuso dei propri poteri a favore della promozione degli interessi nazionali e a scapito, invece, della tutela dei diritti dell'uomo e delle libertà fondamentali. Lo stesso varrebbe nel caso in cui lo Stato non riesca adeguatamente a garantire, mediante le adeguate

[162] Qui, il ruolo della Corte europea dei diritti dell'uomo è stato fondamentale per capire quali sono gli atti nazionali riconducibili alla nozione di 'legge'. Nella sentenza del 25 febbraio 1992, n. 12963/87: III-n80, *Margareta e Roger Andersson c. Svezia*, si afferma: "l'espressione «previste dalla legge», richiede, anzitutto, che la misura contestata abbia una base in diritto interno, ma concerne anche la qualità della legge in questione: ne richiede l'accessibilità agli interessati e una formulazione molto precisa per consentire loro avvalendosi, se del caso, di pareri specialistici di prevedere, ad un livello ragionevole nelle circostanze di causa, le conseguenze che possono scaturire da una determinata azione. Una legge che conferisce un potere discrezionale non contrasta di per sé con tale requisito, a condizione che l'estensione e le modalità d'esercizio di simile potere siano definite con sufficiente chiarezza, considerato lo scopo legittimo in gioco, per fornire all'individuo una protezione adeguata contro l'arbitrio".
[163] Sentenza della Corte europea dei diritti dell'uomo dell'8 giugno 1976, n. 22, *Engel e altri c. Paesi Bassi*.
[164] Le autorità nazionali nel disporre formalità, condizioni, restrizioni o sanzioni all'esercizio della libertà di espressione devono sempre indicare espressamente la motivazione alla base delle medesime in modo pertinente e sufficiente, al fine di consentire di effettuare un vaglio della loro legittimità in sede giurisdizionale nazionale e comunitaria (Sentenza della Corte europea dei diritti dell'uomo del 15 marzo 2002, n. 46833/99, *Nafria c. Spagna*).

misure di prevenzione e protezione, una corretta tutela dei diritti umani rispetto ad attacchi esterni che egualmente violerebbero i dettami della Convenzione.
In più, la Corte ha aggiunto che qualsiasi misura restrittiva debba essere chiaramente definita nelle sue modalità, nel suo scopo e nella sua durata, in modo da rendere di facile individuazione il tipo di contenuto che sarà bloccato, e perciò reso inaccessibile, l'area geografica entro la quale tali misure saranno valide e il periodo durante il quale questa troverà applicazione. La Corte riconosce, inoltre, agli Stati un certo margine di discrezionalità rispetto alla sussistenza di questo bisogno ma afferma, nel contempo, che spetta alla stessa valutare la situazione sociale contingente in cui tali misure restrittive vengono prese e stabilirne la liceità[165].
Ancora, essa ha stabilito chiaramente che qualsiasi restrizione da parte dello stato deve essere proporzionale rispetto all'interesse pubblico prioritario che s'intende salvaguardare. Il rispetto del principio di proporzionalità implica anche la non ammissibilità di restrizioni da parte dello stato tutte le volte in cui un altro tipo di azione meno restrittiva (non incidente sulla libertà di espressione) possa servire al perseguimento del medesimo obiettivo[166].
Infine, deve esserci un chiaro e trasparente processo di implementazione di tali misure e una notifica nei confronti di coloro verso le quali esse sono indirizzate, nonché la previsione di meccanismi che garantiscano la possibilità di effettuare appelli e ricorsi giudiziari.
Va da sé, dunque, che qualsiasi

> indiscriminate blocking measure which interferes with lawful content, sites or platforms as a collateral effect of a measure aimed at illegal content or an illegal site or platform would not be legal, and blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship[167].

Date queste premesse, esaminiamo due casi pertinenti presentati presso la Corte europea dei diritti dell'uomo con lo scopo di cogliere gli aspetti essenziali del ragionamento logico-giuridico alla base delle sentenze della stessa.
La prima sentenza che analizzeremo è quella relativa al caso *Delfi AS c. Estonia* pronunciata dalla Camera in prima sezione della Corte europea dei diritti dell'uomo. In essa sono emerse due esigenze fondamentali in materia di tutela della libertà di espressione in Internet: da un lato, la protezione della

[165] Sentenza della Corte europea dei diritti dell'uomo del 17 luglio 2008, n. 42211, *Riolo c. Italia*.
[166] Sentenza della Corte europea dei diritti umani del 17 luglio 2007, ricorso n. 36109, *Ormanni c. Italia*.
[167] Sentenza della Corte europea dei diritti umani del 18 marzo 2013, 3111/10, *Ahmet Yıldırım c. Turchia*.

libertà di espressione in rete e dei relativi diritti dei suoi utenti; dall'altro, la protezione dell'onore e della reputazione delle persone[168].

Il caso può essere riassunto come segue.

La ricorrente è la società proprietaria di 'Delfi', uno dei più grandi portali Internet di notizie in Estonia[169].

Il portale pubblicava, all'epoca dei fatti, fino a 330 articoli di notizie al giorno. I lettori potevano, inoltre, postare e leggere, sul portale Internet, i relativi commenti agli articoli pubblicati.

Ai tempi dei fatti in questione, i commenti (circa 10000 al giorno[170]) erano caricati automaticamente, non erano né editati né moderati dalla società ricorrente; in più, nella maggioranza dei casi, erano postati sotto pseudonimi.

Il portale prevedeva, tuttavia, un sistema che permetteva ad ogni lettore di segnare un commento come *leim*, cioè come un messaggio recante insulti o istigante all'odio su Internet. Se ciò accadeva il commento veniva immediatamente rimosso[171]. Inoltre, il sistema prevedeva la rimozione automatica di commenti che contenevano certe radici di parole oscene.

Oltre a ciò, la vittima di un commento diffamatorio poteva anche direttamente contattare la società ricorrente per richiedere la rimozione del commento[172].

È importante evidenziare, infine, che il Regolamento del sito, il quale rendeva noto agli utenti tale sistema di rimozione automatica, prevedeva che gli autori dei commenti fossero considerati responsabili per il loro contenuto[173].

Secondo quanto riporta la Corte europea dei diritti dell'uomo[174], nel gennaio 2006 la società ricorrente pubblicò, sul portale Delfi, un articolo riguardante le attività di una compagnia marittima che forniva servizi di trasporto pubblico tra il continente e alcune isole che attirò 185 commenti, una ventina dei quali conteneva minacce personali e un linguaggio offensivo nei confronti di L., membro del consiglio di sorveglianza della compagnia marittima.

Successivamente, nel marzo 2006, gli avvocati di L. chiesero alla società ricorrente la rimozione dei commenti offensivi e un risarcimento di circa 32000 euro per danni non patrimoniali. La società ricorrente accettò di

---

[168] Rileva, a tal proposito, il documento adottato dal Comitato dei ministri del Consiglio d'Europa il 28 maggio 2003, *Dichiarazione sulla libertà di comunicazione in Internet*, nel quale si afferma: "The member states of the Council of Europe [...] convinced also that it is necessary to limit the liability of service providers when they act as mere transmitters, or when they, in good faith, provide access to, or host, content from third parties [...]. Stressing that freedom of communication on the Internet should not prejudice the human dignity, human rights and fundamental freedoms of others, especially minors [...]".

[169] SEMINARA (2015: 1).

[170] Sentenza della Corte europea dei diritti dell'uomo del 10 ottobre 2013, *Delfi AS c. Estonia*, ricorso n. 64569/09.

[171] *Ivi*, p. 2.

[172] *Ibidem*.

[173] *Ibidem*.

[174] Sentenza della Corte europea dei diritti dell'uomo del 10 ottobre 2013, *Delfi AS c. Estonia*, ricorso n. 64569/09.

rimuovere i commenti, ma rifiutò di pagare la somma chiesta come risarcimento. A quel punto, L. avviò un'azione civile contro la società ricorrente: le giurisdizioni interne ritennero quest'ultima civilmente responsabile per i commenti diffamatori e assegnarono a favore di L. un risarcimento di 320 euro per danni non patrimoniali.
In seguito a tale decisione, la politica del sito cambiò: non fu più permesso alle persone che avessero postato commenti offensivi, di postare un nuovo commento finché il commentatore non avesse letto e accettato le regole stabilite per pubblicare commenti. Inoltre, la società ricorrente istituì una équipe di moderatori[175].
Essa decise poi di adire la Corte europea dei diritti dell'uomo asserendo che le giurisdizioni interne, ritenendola civilmente responsabile per i commenti diffamatori pubblicati in rete, avevano infranto la sua libertà di espressione (libertà di impartire informazione), come garantita dall'articolo 10 della Convenzione europea dei diritti dell'uomo.
Di tutt'altra opinione era il governo estone, il quale contestava tale argomentazione affermando che non fosse possibile ritenere la società vittima di una violazione dell'art. 10 della Convenzione poiché essa non era stata né l'autrice dei commenti diffamatori (poi eliminati) né la loro fonte divulgatrice.
Al fine di decidere se la condotta delle autorità nazionali, ritenuta affine all'ambito di applicazione dell'articolo 10 della Convenzione, abbia rispettato il diritto sancito da questa disposizione, la Corte dapprima si è accertata che l'ingerenza statale sia stata prevista dalla legge; in secondo luogo, essa ha stabilito che la restrizione applicata dalla società ricorrente perseguiva uno scopo legittimo, e cioè quello di proteggere la reputazione e i diritti di altri individui[176]; l'unica questione che rimaneva da affrontare riguardava il rispetto del requisito della necessità dell'ingerenza in una società democratica.
Il problema era capire se le autorità nazionali fossero riuscite nel perseguimento dell'equilibrio tra due diritti egualmente garantiti all'interno della Convenzione (il diritto al rispetto della propria vita privata, tutelato dall'art. 8; la libertà di espressione, tutelata dall'art. 10) e non avessero, invece, ridotto la tutela dell'uno dando priorità alla protezione dell'altro mediante misure non necessarie.
Per risolvere la questione, la Corte ha analizzato quattro elementi:

---

[175] *Ibidem*.
[176] Sentenza della Corte europea dei diritti dell'uomo del 10 ottobre 2013, *Delfi AS c. Estonia*, ricorso n. 64569/09: "The Court considers that the restriction of the applicant company's freedom of expression pursued a legitimate aim of protecting the reputation and rights of others. The Court has taken note of the applicant company's argument about the liability of the actual authors of the comments. However, in the Court's view the fact that the actual authors were also in principle liable does not remove the legitimate aim of holding the applicant company liable for any damage to the reputation and rights of others. The question of whether the applicant company's rights under Article 10 were excessively restricted in the present case by holding it liable for comments written by third parties is a question of whether the restriction was 'necessary in a democratic society', to be dealt with below".

1. il contesto dei commenti; a riguardo la Corte stabilisce che la società ricorrente, dati i temi trattati nell'articolo, avrebbe potuto "[…] realise that it might cause negative reactions […][177]" e stimolare la pubblicazione di commenti offensivi. Dunque, ritiene che la società ricorrente avrebbe dovuto/potuto mostrarsi più prudente per evitare di essere ritenuta responsabile per violazione delle norme dirette alla tutela della reputazione di altre persone.
2. le misure adottate dalla società ricorrente al fine di evitare o rimuovere commenti diffamatori. A riguardo, la Corte nota che la società ricorrente aveva provveduto ad instituire dei meccanismi automatici di rimozione dei commenti considerati offensivi, pur essendosi rivelati insufficienti ad impedire danni a terzi, e che, di fatto, esercitava un sostanziale grado di controllo sui commenti pubblicati sul suo portale, non modificabili dagli autori stessi. Infine, consiste essa ritiene fondamentale il fatto che le giurisdizioni interne non abbiano dato ordini alla società ricorrente su come la stessa dovesse assicurare la protezione dei diritti dei terzi, e che avevano fatto ricadere la scelta sulla società ricorrente (la quale aveva agito come meglio credeva).
3. la responsabilità dei reali autori dei commenti come alternativa alla responsabilità della società ricorrente. A tal proposito, la Corte afferma che individuare dichiarazioni diffamatorie e rimuoverle è un compito difficile. Secondo la Corte, è difficile per l'operatore di un portale Internet di notizie, ma è un compito ancora più oneroso per le persone potenzialmente danneggiate che, meno probabilmente avrebbero risorse per monitorare in continuazione Internet.
4. le conseguenze dei procedimenti interni per la società ricorrente, consistenti sostanzialmente nel risarcimento di 320 euro per danno non patrimoniale che la società ricorrente è stata obbligata a pagare alla persona danneggiata. A riguardo, la Corte ritiene che la suddetta somma, tenendo conto del fatto che la società ricorrente sia un operatore professionale di uno dei più grandi portali Internet in Estonia, non è affatto sproporzionata.

In conclusione, secondo il ragionamento della Corte la decisione delle giurisdizioni interne che ha ritenuto responsabile la società ricorrente per i commenti diffamatori postati dai lettori sul suo portale Internet è stata, , una 'restrizione giustificata e proporzionata' del diritto alla libertà di espressione della società ricorrente. Non vi è stata, perciò, violazione dell'articolo 10 della Convenzione[178].
Diversamente, come abbiamo anche avuto modo di dire nelle pagine precedenti, la Corte ha rilevato una violazione del medesimo articolo nel

[177] *Ibidem*.
[178] *Ibidem*.

caso *Yildirim c. Turchia*. Esaminiamo il caso per comprendere il ragionamento che, in tale occasione, ha seguito la Corte.
Il ricorrente, sig. Ahmet Yıldırım, è un cittadino turco, nato nel 1983 e residente a Istanbul. Egli è proprietario e amministratore di un sito Web, ospitato dal servizio '*Google Sites*', sul quale pubblica i suoi lavori accademici ed i suoi punti di vista in svariati ambiti.
Il caso nasce da una decisione del tribunale penale di Denizli, emessa il 23 giugno 2009 mediante la quale ordinava il blocco dell'accesso ad un sito internet il cui proprietario era accusato di oltraggio alla memoria di Atatürk. La decisione di blocco è stata poi notificata per l'esecuzione alla Presidenza delle Telecomunicazioni e dell'Informatica (PTI). Poco dopo, su richiesta di quest'ultima, il tribunale ha riformulato la sua decisione e ha disposto il blocco totale dell'accesso a '*Google Sites*' che ospitava non soltanto il sito terzo, ma anche quello del ricorrente. Questa decisione fu presentata, di fatto, come una misura preventiva adottata nell'ambito di un procedimento penale. Inoltre, La PTI dichiarava che questo era l'unico mezzo tecnico per bloccare il sito in causa, in quanto il suo proprietario risiedeva all'estero.
Nel momento in cui la PTI bloccò totalmente l'accesso a '*Google Sites*', il sig. Yildirim si trovò nell'impossibilità di accedere anche al proprio sito. Tutti i suoi tentativi di ricorso interno risultarono vani[179] ed è per tale ragione che egli ha deciso di rivolgersi alla Corte europea dei diritti dell'uomo, ritenendo che il governo turco stesse violando l'art. 10 della Convenzione europea dei diritti dell'uomo.
Decisa la ricevibilità del caso, la Corte ha osservato che il blocco dell'accesso al sito internet del ricorrente aveva ad origine una decisione del tribunale di Denizli che aveva avviato un procedimento penale a carico del proprietario di un altro sito internet, accusato di oltraggio alla memoria di Atatürk (considerato padre fondatore della Repubblica di Turchia).
Ciò che la Corte si è trovata a giudicare, di fatto, ha riguardato gli effetti collaterali di una misura preventiva adottata nell'ambito di un procedimento giudiziario, che hanno reso impossibile per più di un individuo l'accesso ad Internet: per la Corte questo rientra nell'ambito della sfera di garanzia di cui all'art. 10 della CEDU[180], considerando l'importante ruolo di Internet quale fonte preziosa di informazioni rilevanti per lo sviluppo della propria capacità di opinione ed espressione. Per tale ragione, la Corte identifica l'azione del governo turco come una misura restrittiva della libertà di accesso a tale risorsa.
Precisato questo, essa prosegue il suo ragionamento cercando di determinare, allora, se tale misura sia lecita secondo quanto stabilisce l'art. 15 della Convenzione: tale misura deve, perciò, essere prevista per legge, perseguire uno o più scopi legittimi ed essere necessaria in una società democratica.

[179] Sentenza della Corte europea dei diritti dell'uomo del 18 dicembre 2012, n. 3111/10, *Ahmet Yildirim c. Turchia*.
[180] *Ibidem*.

Per quanto riguarda il primo punto, la Corte osserva che la misura di restrizione dell'accesso ad Internet è stata attuata ai sensi della legge turca n. 5651, in base alla quale un giudice può disporre il blocco dell'accesso alle pubblicazioni diffuse via Internet se ha motivi sufficienti per sospettare che per il loro contenuto costituiscano reato. Tale legge, tuttavia, non fa riferimento ad un blocco integrale di accesso, così come invece ha disposto il tribunale turco. Inoltre, la Corte evidenzia che il tribunale di Denizli non ha verificato se vi fosse la possibilità di adottare una misura meno severa per bloccare nello specifico il sito interessato.
Infine, secondo la Corte, i giudici avrebbero dovuto preoccuparsi che un'estensione di quanto previsto dalla legge n. 5651 avrebbe reso inaccessibile una notevole quantità di informazioni andando a ledere direttamente i diritti di più utenti e producendo, quindi, un effetto collaterale di spiccata rilevanza.
La Corte afferma, inoltre, che la misura restrittiva non persegue alcuno scopo legittimo, che ha avuto degli effetti arbitrari e che non ha adeguatamente assicurato la preminenza del diritto alla libertà di espressione che si esige all'interno di una società democratica.
In ragione di ciò, la Corte conclude che vi è stata una violazione dell'art. 10 e dichiara la Turchia responsabile. Essa stabilisce, inoltre, il versamento al ricorrente di un'equa soddisfazione pari alla somma di 7.500 euro per danni morali e 1000 euro per spese[181].

Dunque, abbiamo visto come la Corte è arrivata a determinare se e quando vi sia stata una violazione del diritto alla libertà di espressione nel contesto *cyber* alla luce della Convenzione europea dei diritti dell'uomo, tenendo anche conto di tutti gli altri documenti internazionali in materia.
Di fatto, gli attuali strumenti giuridici in materia di diritti umani consentono una certa flessibilità nell'applicazione di tali norme al contesto cibernetico offrendo agli individui un quadro normativo tale da consentire, anche in rete, un'adeguata protezione dei propri diritti.
Con particolare riferimento al rispetto del diritto alla libertà di espressione possiamo affermare che eventuali restrizioni al libero accesso alla rete, approvate volontariamente dagli Stati (qualsiasi sia il loro scopo) o determinate da attacchi informatici quali DDoS, che abbiamo analizzato nel primo capitolo (e i cui effetti sono pressoché i medesimi se non più gravi, essendo essi degli attacchi mirati proprio a bloccare un computer o una rete con lo scopo di ostacolare il libero accesso agli utenti), sono comunque soggette alle norme internazionali in materia di diritti umani, il cui rispetto deve essere, pertanto, promosso anche all'interno del *cyber space.*
In tale contesto, altrettanto rilevante è il diritto alla *privacy*, corollario alla libertà di espressione e da intendere tanto come diritto di non interferenza nella vita privata del singolo quanto come diritto alla protezione di tutte quelle informazioni riguardanti tale sfera personale.

[181] *Ibidem.*

Il diritto alla privacy

Per quanto riguarda le norme a livello internazionale, tale diritto è contenuto sia nella Dichiarazione universale del 1948, all'art. 12[182], sia nel Patto sui diritti civili e politici del 1966, all'art. 17[183], entrambi i quali tutelano l'individuo contro interferenze arbitrarie nella sua sfera privata.

Sul piano regionale invece, rileva l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nel quale si attesta che:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Data l'importanza del tema, soprattutto negli ultimi anni numerosi Stati hanno provveduto a ridefinire il quadro normativo in materia di tutela alla riservatezza. Fra questi, spicca l'Italia: infatti, mediante l'approvazione del c.d. Codice della *privacy* nel 2003 (modificato dal Decreto legislativo del 14 settembre 2015, n. 151 e, successivamente, dalla Legge del 7 luglio 2016, n. 122) il Paese ha esplicitamente riconosciuto l'importanza di tale diritto. Esaminiamo, dunque, il suo contenuto al fine di delineare, in linea generale, le specificità del modello di tutela della *privacy* italiano.
Il Codice si compone di tre parti:
La prima parte contiene un insieme di disposizioni generali (art. 1-45) relativi alle regole 'sostanziali' della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, salvo eventuali regole specifiche per i trattamenti effettuati da soggetti pubblici o privati (art. 6).
La seconda parte contiene diverse disposizioni particolari per specifici trattamenti (articoli. 46-140) ad integrazione o eccezione alle disposizioni generali della parte I.
Infine, la terza parte racchiude tutte le disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio (articoli 141-186).
A queste seguono tre allegati:

[182] Dichiarazione universale del 1948, art. 12: "No one shall be subjected to arbitrary interference with his *privacy,* family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".
[183] Patto internazionale sui diritti civili e politici del 1966, art. 17: "No one shall be subjected to arbitrary or unlawful interference with his *privacy*, family, home or correspondence, nor to unlawful attacks on his honour and reputation.".

- allegato A, relativo ai codici di condotta;
- allegato B, concernente il disciplinare tecnico in materia di misure minime di sicurezza;
- allegato C, sui trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia.

Il Codice prevede sia il diritto a non vedere trattati i propri dati senza consenso e sia l'adozione di misure cautelari di tipo tecnico ed organizzativo da rispettare per procedere in maniera corretta al trattamento dei dati altrui.
Alla base del Codice troviamo due principi cardine: il primo principio è il principio di origine o stabilimento, in base al quale è disciplinato il trattamento dei dati personali, anche detenuti all'estero, effettuato da chiunque abbia sede nel territorio italiano, o in uno Stato non appartenete all'Unione europea; il secondo principio è il principio di ubicazione degli strumenti elettronici, che riguarda gli strumenti impiegati per il trattamento dei dati personali che debbono essere in ogni caso situati nel territorio italiano.
L'obiettivo primario che ha portato all'adozione del Codice della *privacy* è quello di minimizzare i rischi di perdita e distruzione dei dati, perseguito mediante la disciplina delle misure di sicurezza 'minime' che devono essere adottate da chiunque tratti dati personali altrui.
Ciò detto, cerchiamo di capire cosa si intende con l'espressione dati personali.
Per 'dato personale' si intende

> qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale[184].

Il decreto legge 6 dicembre 2011, n. 201 (convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214) , modificando la lettera della norma, ha escluso che nella definizione di dato personale rientrassero le informazioni delle persone giuridiche, che di norma possono quindi essere trattate liberamente.
Per quanto riguarda le caratteristiche distintive dei dati personali, possiamo distinguere tre macro categorie:

1. *dati identificativi*, che permettono l'identificazione diretta dell'interessato;
2. *dati sensibili*, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,

[184] *Codice in materia di protezione dei dati personali*, decreto legislativo del 30 giugno 2003, n. 196.

nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
3. *dati giudiziari*, idonei invece a rivelare provvedimenti carico, casellario giudiziario, sanzioni e via dicendo[185].

Entrando nel merito del Codice, esso stabilisce che il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato, che può riguardare l'intero trattamento oppure una o più operazioni dello stesso; inoltre, è stabilito che la sua validità si attesta soltanto laddove questo sia espresso liberamente e in riferimento ad un trattamento chiaramente individuato.
Un'ulteriore doverosa precisazione riguarda i dati sensibili: fermo restando le condizioni necessarie per la validità del consenso al trattamento dei dati appena specificate, per i dati sensibili è necessaria la forma scritta.
Ciò detto, risulta importante individuare i soggetti nei confronti dei quali il Codice si rivolge. Questi sono cinque:

1. il *titolare*, ovvero la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza[186];
2. l' *interessato*, la persona fisica cui si riferiscono i dati personali[187];
3. il *responsabile*, ossia la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali[188];
4. gli *incaricati*, cioè le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile[189];
5. il *Garante*. Al fine di controllare la corretta applicazione della normativa in materia di *privacy* è stato istituita, per l'appunto, tale apposita autorità amministrativa indipendente avente il compito di assicurare il rispetto della disciplina sulla riservatezza previsto dalla legge tramite poteri istruttori, consultivi e sanzionatori. Egli ha il compito di verificare e controllare il trattamento dei dati da parte del responsabile o del titolare e può, ove necessario, disporre anche sanzioni amministrative. Inoltre, tale figura prescrive al titolare le opportune misure per rendere il trattamento dei dati conforme alle disposizioni vigenti[190].

---

[185] *Codice in materia di protezione dei dati personali*, decreto legislativo del 30 giugno 2003, n. 196, art. 4.
[186] *Ibidem*.
[187] *Ibidem*.
[188] *Ibidem*.
[189] *Ibidem*.
[190] *Ivi*, art. 153.

Il diritto alla *privacy* perciò, così come elaborato all'interno del Codice, non è da intendersi soltanto come un diritto a non vedere trattati i propri dati senza consenso ma comprende anche l'adozione di adeguate misure di cautela al fine di procedere ad un corretto trattamento dei dati personali.
Il Codice fornisce anche un'utile definizione di 'trattamento', inteso come

> qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati[191].

Si stabilisce inoltre che, ai fini di un corretto trattamento dei dati personali, sia importante ridurre per quanto possibile l'utilizzo o l'archiviazione di grandi quantità di dati personali ed identificativi, cercando di utilizzare dati anonimi o di impiegare dati personali soltanto in caso di necessità[192].
Accanto alle sanzioni amministrative eventualmente decise dal Garante, possono essere comminate anche sanzioni di tipo penale e civile.
Le prime si dividono in:

- misure minime, previste dall'art. 33; qualora esse non vengano adottate è previsto un arresto fino a due anni.
- trattamento illecito (previsto dall'art. 167); laddove qualcuno procedesse al trattamento dei dati personali in violazione di alcuni articoli del Codice, al fine di trarne profitto, egli sarà punito con la reclusione dai 6 agli 8 mesi oppure, se il fatto avvenisse nell'ambito della comunicazione o diffusione, con una sanzione pari a 6 o 24 mesi di reclusione.

Per quel che concerne la responsabilità civile per danni, il Codice *privacy* qualifica il trattamento dei dati personali come attività pericolosa, ex. art. 2050 c.c., ed è da evidenziare come ciò comporti un'inversione dell'onere della prova nell'azione risarcitoria, per cui tale onere viene a gravare sull'azienda o sull'ente, che sono tenuti a dimostrare di avere applicato tutte le misure di sicurezza più idonee a garantire la sicurezza dei dati personali gestiti. Tali misure devono essere finalizzate alla riduzione dei rischi di perdita, distruzione, sottrazione o manipolazione dei dati personali.

Come abbiamo visto nel primo capitolo, analizzando il caso della 'JP Morgan Chase & Co', nel contesto delle reti informatiche, il diritto alla *privacy* ha assunto sempre più importanza. In fatti, nel *cyber* spazio la diffusione di dati è incredibilmente semplice e veloce e, tuttavia, numerose sono le vulnerabilità dei sistemi informativi che rendono altrettanto facile la

[191] *Ivi*, art. 4.
[192] *Ivi*, art. 22.

loro manipolazione o il loro furto.
Nondimeno, spesso le politiche di *cyber security* attuate da alcuni Stati sembrano confliggere con la tutela del diritto alla riservatezza.
Nei prossimi paragrafi, analizzeremo nel dettaglio la questione e cercheremo di avvalorare la tesi secondo cui è, invece, la protezione dei dati essenziale presupposto per una efficace politica di *cyber security*.

3.4 *Privacy* vs Sicurezza

La tutela della *privacy* è un concetto fondamentale all'interno delle società democratiche, una garanzia che ha assunto ormai una posizione di rilievo. Eppure, questa stessa società posta di fronte a nuove sfide come quelle lanciate dal *cyber space* sta mettendo in discussione uno dei suoi principi cardine in nome di un altro concetto assai rilevante, quello di sicurezza. Ciò nonostante, tali società sanno che occorre trovare un equilibrio tra la ricerca di maggiore sicurezza e il diritto alla riservatezza.
Il problema che a questo punto sorge non riguarda, allora, la legittimità delle azioni di un governo tese a raccogliere e intercettare dati o informazioni personali ma se le modalità attraverso cui questo avviene siano lecite, proporzionali alla minaccia oggettiva e commisurate al rischio a cui si è esposti (e che si vuole ridurre).
Generalmente, si ritiene che uno Stato possa violare il diritto alla *privacy* se:

1. esiste una norma costituzionale che lo permette;
2. la misura che viene adottata è proporzionata al danno che si vuole impedire e le sue conseguenze future;
3. la misura sia adeguata poiché quella è l'unica via per raggiungere lo scopo desiderato.

Solo e soltanto quando ciò avviene possiamo ritenere che sia legittimo, in nome della sicurezza, porre dei limiti all'esercizio di diritto fondamentali come quello a protezione della riservatezza.
Con l'avvento di Internet e la produzione di nuove modalità di raccolta dati mediante l'impiego di strumenti informatici si è fatta strada una nuova concezione di tale diritto che estende o comunque declina in termini più ampi il concetto di riservatezza, non più intesa solo come una sorta di 'diritto ad essere lasciati soli' ma come garanzia di non diffusione di dati, fatti o informazioni appartenenti alla sfera privata e personale di un individuo.
Tuttavia, alcuni ritengono che la protezione della riservatezza possa costituire un ostacolo alla realizzazione di efficaci politiche di sicurezza, pubblica e nazionale.
Prendiamo ad esempio il fenomeno, tanto discusso, della videosorveglianza. Essa nasce a fronte di due particolari esigenze: la prima è riconducibile al bisogno di garantire una sicurezza pubblica e urbana attraverso azioni di prevenzione e controllo dei fenomeni criminosi e vandalici sia in luoghi pubblici sia in luoghi privati; la seconda, consiste nella volontà di monitorare quanto accade per lo più nelle aziende, a tutela del personale lavorativo ma anche dello stesso patrimonio aziendale.
Ora, la questione principale è che le immagini tracciate dalle videocamere sono pienamente qualificabili come dati personali, dal momento che rendono possibile l'identificazione di ogni singolo individuo[193].

[193] CALIFANO (2013: 21 ss.).

Molti sostengono che una tale violazione della *privacy* sia necessaria a fronte di un bisogno superiore, e cioè una maggiore sicurezza. D'altro canto, non poche persone dissentono obiettando che i dati identificativi di un individuo non possono essere prelevati e diffusi con così estrema facilità.
Questa costante tensione tra *privacy* e sicurezza si riflette anche nell'ambito delle aziende private e non soltanto in ambito di pubblico interesse.
Per capire meglio, pensiamo al fatto che molte delle minacce che le aziende devono affrontare hanno origine all'interno delle stesse e provengono dai loro impiegati. Tale considerazione ci spiega, allora, le ragioni alla base della recente tendenza di molte imprese di monitorare il proprio personale, con un'attenzione particolare ai movimenti che tali persone effettuano in rete. Sebbene tale propensione alla sorveglianza sia in crescita, i sistemi giudiziari nazionali persistono nel riconoscere agli individui (e, nel caso specifico, agli impiegati) la possibilità di rivendicare, anche sul posto di lavoro, il proprio diritto alla riservatezza.
Recentemente, anche la Corte europea dei diritti dell'uomo, nel giudizio sul ricorso n. 61496/08 del 5 settembre 2017 relativo al caso *Bărbulescu c. Romania*, si è espressa in tal senso.
Nel caso in esame, il ricorrente Bogdan Mihai Bărbulescu, nato nel 1979 e residente a Bucarest, era un impiegato presso una società privata rumena come ingegnere di vendita. Su richiesta del suo datore di lavoro, al fine di rispondere alle richieste dei clienti, aveva creato un account di messaggistica istantanea utilizzando Yahoo! Messenger, una trasmissione in tempo reale di testo *on-line* che offre servizio di chat su internet.
I Regolamenti interni del datore di lavoro proibivano l'uso personale di tale account ma non contenevano alcun riferimento alla possibilità per il datore di monitorare le comunicazioni (e, pertanto, le modalità di utilizzo di tale account) dei propri dipendenti. Quando il datore di lavoro ha informato il sig. Bărbulescu che tale attività di monitoraggio effettivamente portata a termine dall'azienda aveva reso noto l'utilizzo improprio da parte dell'impiegato dell'account professionale, egli è stato licenziato sulla base di quanto sancito nei Regolamenti interni all'azienda, e cioè che:

> it is strictly forbidden to disturb order and discipline within the company's premises and especially [...] to use computers, photocopiers, telephones, telex and fax machines for personal purposes[194].

Il ricorrente ha contestato il licenziamento presso i tribunali nazionali, i quali tuttavia hanno respinto il ricorso e hanno confermato la sua legittimità a fronte di quanto sancito dai Regolamenti interni dell'azienda.
A questo punto, il sig. Bărbulescu si è rivolto alla Corte europea dei diritti dell'uomo, che ha accolto il ricorso e stabilito la pertinenza con l'art. 8 della CEDU.

[194] Sentenza della Corte europea dei diritti dell'uomo del 12 gennaio 2016, n. 61496/08, *Bărbulescu c. Romania*.

La Corte di Strasburgo ha evidenziato che la questione principale riguardava il conflitto tra il diritto alla riservatezza del sig. Bărbulescu e la tutela degli interessi del suo datore di lavoro e della sua società.
Nella decisione del 12 Gennaio 2016 la Corte ha negato (con sei voti contro uno) la sussistenza di una violazione dell'art. 8 della Convenzione, ritenendo legittimo il bilanciamento operato dalle Corti nazionali fra la *privacy* del sig. Bărbulescu e gli interessi del datore di lavoro e, dunque, la ragionevolezza del monitoraggio delle comunicazioni del dipendente nel contesto dell'esercizio del potere disciplinare[195].
Il 6 Giugno 2017 la questione viene riferita alla Grande Camera della Corte, su richiesta del ricorrente, la quale invece conferma la sussistenza della violazione dell'art. 8 della Convenzione, che le autorità nazionali non hanno saputo salvaguardare.
La Corte conclude che le comunicazioni sul posto di lavoro rientrino nella tutela di cui all'art. 8 della Convenzione (più precisamente nei concetti di 'vita privata' e 'corrispondenza'). Secondo la Corte le proprie comunicazioni personali possono essere soggette a limitazioni, ma non totalmente[196], ma è necessario che il dipendente sia informato delle eventuali attività di monitoraggio che l'azienda può eseguire circa la propria corrispondenza e della possibilità che i loro risultati siano trasmessi al proprio datore di lavoro.
La Corte ha tenuto a precisare, però, che tali attività di monitoraggio devono comunque rispettare i criteri di necessità e proporzionalità di modo che si evitino i controlli troppo invasivi e non concretamente connessi con le esigenze di sicurezza delle aziende[197].
Tale sentenza dimostra che appare necessario trovare un equilibrio tra la tutela del diritto alla riservatezza e le esigenze di un'azienda, soprattutto quando queste hanno a che fare con la sua sicurezza e quella dei suoi *assets*.
Si potrebbe pensare, tuttavia, che la necessità di assicurare la *privacy* dei propri indipendenti possa costringere le aziende ad indebolire i propri sistemi di sicurezza, non potendo questi sorvegliare oltre certi limiti ciò che accade internamente. La questione si pone, a volte, anche diversamente: potrebbe essere l'azienda stessa a non voler violare la *privacy* dei propri dipendenti o clienti in nome di un bisogno considerato preminente, quale ad esempio la sicurezza nazionale. Ad aver recentemente posto l'attenzione su tale dilemma è stato il c.d. 'caso Apple'.

[195] Sentenza della Corte europea dei diritti dell'uomo del 12 gennaio 2016, n. 61496/08, *Bărbulescu c. Romania*.
[196] Sentenza della Corte europea dei diritti dell'uomo del 5 settembre 2017, n. 61496/08, *Bărbulescu c. Romania*.
[197] *Ibidem*.

Il caso Apple

L'Apple è una delle aziende statunitensi più note nel settore dei sistemi operativi, computer e dispositivi multimediali. Fondata nel 1976 da Steve Jobs, Steve Wozniak e Ronald Wayne, a Cupertino, nella Silicon Valley, in California, è oggi un pilastro nel mondo della tecnologia.
Esaminando quanto accaduto tra Apple e l'FBI nel febbraio 2016 cercheremo di evidenziare gli aspetti più critici riguardanti il presunto conflitto tra *privacy* e sicurezza.
La vicenda vede l'FBI chiedere all'azienda statunitense un aiuto per entrare nel dispositivo personale (IPhone) di Syed Rizwan Farook, uno dei due attentatori della Strage di San Bernardino nel 2015[198], al fine di accedere ai suoi contenuti (cifrati). La risposta dell'Apple è stata piuttosto chiara e dura: la compagnia ha negato tale possibilità affermando che la richiesta di sbloccare il dispositivo e, dunque, disattivare i meccanismi di protezione e sicurezza che prevedono l'inserimento di una password, ovviamente non nota né all'FBI né all'Apple, non era esaudibile[199].
La ragione principale per cui l'FBI ha chiesto il supporto dell'azienda risiede nella caratteristica principale dei suoi dispositivi informatici e cioè la messa in moto di un meccanismo di autodistruzione dei dati qualora si superino i dieci tentativi per entrare nello stesso. La richiesta dell'FBI era, peraltro, molto raffinata: si chiedeva all'Apple di creare una c.d. '*backdoor*' (ossia un accesso secondario per entrare nel sistema aggirando i suoi sistemi di identificazione e protezione) che potesse essere istallata sull'IPhone sottoposto ad indagine. L'Apple ha rifiutato per ovvie ragioni. Creare un simile sistema da un lato, renderebbe chiara a tutti l'esistenza della possibilità di aggirare quei sistemi di protezione che fanno dei dispositivi Apple dei prodotti così appetibili; dall'altro, occorre considerare che, laddove un tale progetto (che ad oggi non esiste) finisse nelle mani sbagliate, tutti i dispositivi Apple potrebbero essere sbloccati facilmente, con conseguenze disastrose per la compagnia e per gli utenti.
Un ulteriore timore della compagnia riguardava il fatto che acconsentire ad una simile richiesta negli Stati Uniti avrebbe potuto costituire il precedente[200] per richieste ancor più compromettenti anche da parte di altri Paesi.

---

[198] Si fa riferimento a quanto accaduto mercoledì 2 dicembre 2015 a San Bernardino, in California. Come riportano i giornali, marito e moglie (rispettivamente riconosciuti nelle persone di Syed Rizwan Farook e Tashfeen Malik) si sono recati presso un centro sociale per disabili, mascherati e armati di fucili, e hanno aperto il fuoco contro le persone presenti, uccidendone all'istante 14 e ferendone altre 24, tra cui due poliziotti. I due attentatori sono deceduti, poi, in seguito ad uno scontro a fuoco con la polizia a 2 km dal luogo della strage. NAGOURNEY, LOVETT e PÉREZ-PEÑA, *San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead*, 2 dicembre 2015, New York Times, reperibile *on-line*.
[199] RIFFAT (2016: 12 ss.).
[200] Lo stare decisis ('rimanere su quanto deciso') è un principio generale dei sistemi di common law, in forza del quale il giudice è obbligato a conformarsi alla decisione adottata in una precedente sentenza, nel caso in cui la fattispecie portata al suo esame sia identica a

La questione di fondo, qui evidenziata, consiste nell'apparente difficoltà di conciliare la tutela del diritto alla *privacy* con la necessità di ottenere sempre più informazioni personali sugli individui (specie se parliamo di terroristi), giudicate necessarie per garantire una maggiore sicurezza nel Paese.
Ciò che bisogna capire, tuttavia, è se la richiesta dell'FBI, dal punto di vista giuridico, possa essere considerata legittima alla luce del principio di proporzionalità. In altre parole, ci si chiede se lo sforzo richiesto all'azienda per '*bypassare'* i meccanismi di protezione (mediante la realizzazione di una *backdoor*) sia proporzionale all'utilità che si ricaverebbe venendo in possesso dei dati contenuti nel dispositivo in questione. La posizione dell'FBI a riguardo è facilmente intuibile[201]. Si crede, infatti, che i dati contenuti nell'IPhone di Farook potessero rivelare informazioni utili a prevenire altri attentati e a scoprire un eventuale rete terroristica *in loco*. Ciò nonostante, l'azienda ha avuto effettivamente la facoltà di negare l'accesso a tali dati.
La questione si è poi risolta diversamente: l'FBI è riuscita a violare i sistemi di sicurezza dell'IPhone e ad accedere ai dati ivi contenuti senza l'aiuto di Apple (mai è stata, tuttavia, rilasciata una dichiarazione riguardante le specifiche modalità attraverso cui ciò è avvenuto), raggiungendo così il proprio obiettivo. Dal canto suo, Apple per il momento è riuscita a ridurre i danni che un tale evento poteva provocare all'azienda.
Al di là dei risvolti è, comunque, importante riflettere sulla vicenda poiché ci sono almeno tre considerazioni da fare.
La prima riguarda la possibilità per cui Apple, così come altre aziende, possano decidere di elaborare sofisticati sistemi di protezione e di sicurezza che neanche esse stesse sarebbero in grado di violare in modo da impedire che richieste come quella fatta dall'FBI possano essere nuovamente presentate e per far sì che le persone percepiscano l'effettiva offerta di una maggiore tutela dei propri dati personali da parte della compagnia.
La seconda considerazione riguarda gli eventuali danni a livello reputazionale che l'azienda Apple avrebbe subito, una volta dimostrata la possibilità di aggirare i sistemi di sicurezza dei suoi dispositivi. Con tutta probabilità, Apple sarà interessata a conoscere i dettagli concernenti le modalità tramite le quali si è riusciti a violare il meccanismo di sicurezza dell'IPhone, in modo da poter sviluppare sistemi più sicuri e garantire l'inviolabilità dei dispositivi agli utenti che ne fanno uso.
Infine, occorre riflettere sulla probabilità per cui gli Stati possono decidere di obbligare le aziende a sviluppare servizi di intrusione nei dispositivi informatici in caso di necessità sulla base della convinzione che, in casi specifici, questo sia decisivo per acquisire tutte le informazioni necessarie ad offrire una maggiore sicurezza ai propri cittadini. L'idea di fondo è che

---

quella già trattata nel caso in essa deciso. In questo modo, i precedenti desunti dalle sentenze anteriori operano come fonte di diritto e, negli ordinamenti di common law, a tutt'oggi, la maggior parte delle norme è prodotta proprio tramite questa fonte.
MORBIDELLI, PEGORARO, RINELLA, VOLPI (2016: 63).
[201] RIFFAT (2016: 14 ss).

un'eccessiva tutela della riservatezza comporti evidentemente un decremento della capacità di garantire sicurezza a causa della scarsità delle informazioni in possesso alle autorità competenti. Viceversa, una maggiore sicurezza richiede una limitazione del diritto alla *privacy* e il libero accesso a dati e informazioni personali diversamente protette.

Oggigiorno si sta facendo strada, dunque, l'idea che la *privacy* debba cedere il passo alla sicurezza e che per garantire protezione ai propri cittadini sia necessario apporre restrizioni ad alcuni diritti e libertà individuali (come il diritto alla *privacy*). Non appare del tutto impossibile percorrere, invece, un'altra strada.
Nel prossimo paragrafo vedremo come mediante un controllo sempre più efficiente circa il trattamento dei dati personali è possibile garantire al contempo la tutela della riservatezza degli utenti e una maggiore sicurezza nazionale e delle reti informatiche, che si realizza proprio grazie ad un costante monitoraggio delle eventuali violazioni dei dati personali e all'attuazione di adeguati meccanismi di pronta risposta e prevenzione.
A riguardo, la recente disciplina dell'Unione europea sembra offrire un modello da imitare.

3.5 Dalla Carta di Nizza al General Data Protection Regulation

Tra gli obiettivi dell'Unione europea rientra, infatti anche quello di assicurare l'applicazione sistematica del diritto alla protezione dei dati, che trova una sua base giuridica nella Carta dei diritti fondamentali dell'Unione europea (nota anche come Carta di Nizza, solennemente proclamata il 7 dicembre 2000) e nel Trattato sul funzionamento dell'Unione europea (che insieme al Trattato sull'Unione europea costituisce le basi fondamentali del diritto europeo).
Enunciamo brevemente gli articoli della Carta di Nizza in materia, e cioè l'art. 7, il quale afferma che: "Everyone has the right to respect for his or her private and family life, home and communications"[202] e l'art. 8, relativo alla protezione dei dati. Quest'ultimo stabilisce che

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

Ricordiamo che con l'entrata in vigore del Trattato di Lisbona la Carta è stata riconosciuta come uno strumento giuridicamente vincolante per l'Unione, le sue istituzioni, i suoi organi e per gli Stati membri in quanto ormai parte del diritto dell'Unione europea.
Per quanto riguarda il TFUE, invece, è mediante l'art. 16 che si assegna a Parlamento e Consiglio il compito di stabilire le norme relative alla protezione delle persone fisiche in merito al trattamento dei dati di carattere personale, da parte delle istituzioni, degli organi e delle agenzie dell'Unione, nonché da parte degli Stati membri nell'esercizio delle attività che rientrano nel campo di applicazione del diritto dell'Unione[203].
Con l'approvazione del Trattato di Lisbona del 2007 è venuta meno la divisione in tre pilastri del diritto comunitario, che in materia di protezione dei dati personali nello spazio di libertà, sicurezza e giustizia era divisa tra il primo pilastro (protezione dei dati a fini privati e commerciali, soggetta al

[202] Carta dei diritti fondamentali dell'Unione europea, Nizza, 7 dicembre 2000.
[203] Trattato sul funzionamento dell'Unione europea, Roma, 25 marzo 1957, art. 16:
"Everyone has the right to the protection of personal data concerning them.
The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union".

metodo comunitario) e il terzo pilastro (protezione dei dati per scopi di ordine pubblico, con decisioni prese a livello intergovernativo). Di conseguenza, il processo decisionale seguiva due diversi insiemi di norme. Tuttavia, sebbene questa struttura non esista più, persistono ancora una serie di strumenti giuridici diversi, tra cui le direttive europee nell'ambito dell'ex primo pilastro, come la direttiva 95/46/CE sulla protezione dei dati, la direttiva 2002/58/CE sull'e-*privacy*, modificata nel 2009, la direttiva 2006/24/CE sulla conservazione dei dati (dichiarata invalida dalla Corte di giustizia dell'Unione europea l'8 aprile 2014 a causa delle gravi interferenze con la vita privata e la protezione dei dati personali), il regolamento (CE) n. 45/2001 sul trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari nonché, nell'ambito dell'ex terzo pilastro, la decisione quadro del Consiglio del novembre 2008 sulla protezione dei dati personali trattati nell'ambito della polizia e della giustizia penale.
Ad ogni modo, l'Unione europea non ha arrestato il processo evolutivo in materia e, di fatto, ha elaborato nuovi atti, alcuni dei quali modificheranno nel prossimo futuro il *frame work* legale esistente mediante l'abrogazione di alcune delle norme al momento vigenti e l'introduzione di una nuova disciplina giuridica.
Rilevante a tal proposito è l'approvazione da parte del Parlamento europeo e del Consiglio del regolamento del 27 aprile 2016, n. 679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, che abrogherà la direttiva 95/46/CE.
Altrettanto importante è la direttiva del Parlamento europeo e del Consiglio, del 27 aprile 2016, n.680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, la quale abrogherà la decisione quadro 2008/977/GAI del Consiglio che disciplina la protezione dei dati (giudiziari e di polizia scambiati tra Stati membri e autorità e sistemi dell'UE) nell'ambito dell'ex terzo pilastro.
Esaminiamo in maniera più approfondita entrambi i documenti.

Il regolamento del 27 aprile 2016, n. 679

Tale regolamento segna una tappa importante del percorso europeo verso una efficace armonizzazione delle regole relative alla protezione della *privacy* e, insieme alla direttiva (UE) 2016/680, costituisce il c.d. 'pacchetto protezione dati personali'.
Il regolamento è entrato in vigore il 24 maggio 2016 ma troverà applicazione negli Stati solo alla data del 25 maggio 2018: le imprese e le pubbliche amministrazioni di ogni Stato membro dell'Unione europea hanno, pertanto, un periodo di tempo pari a due anni per adeguarsi alla disciplina da esso stabilita e attuare le misure necessarie a garantire un corretto trattamento dei dati.

Il testo del regolamento, come già detto precedentemente, abroga la direttiva 95/46/CE in materia di protezione dei dati personali, concepita in un periodo nel quale solo una minima parte della popolazione europea utilizzava Internet[204]; inoltre, non esistevano ancora piattaforme digitali quali *social media* o dispositivi come *smartphones* e *tablet* grazie ai quali gli utenti si potevano connettere alle reti informatiche e pubblicare, più o meno inconsapevolmente, i propri dati personali[205].
Esaminiamo, allora, gli elementi salienti del regolamento ed evidenziamo le novità da esso introdotte.
Il testo del regolamento riconosce un livello elevato e uniforme di tutela dei dati personali e si pone come fine ultimo quello di offrire ai cittadini europei un maggiore controllo di questi ultimi. Esso, inoltre, pone i cittadini e i loro diritti in primo piano e, in sintesi, riconosce loro:

- il diritto alla portabilità dei dati (art. 20), ossia il diritto a ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i propri dati personali forniti ad un titolare del trattamento e il diritto di trasmettere tali dati ad un altro titolare senza impedimenti;
- il diritto all'oblio, riconosciuto fino ad ora solo a livello giurisprudenziale, che prevede il diritto di ottenere dal titolare del trattamento la cancellazione dei propri dati personali senza ingiustificato trattamento se sussiste uno dei motivi elencati all'art. 17 del regolamento[206];
- il diritto di essere informato in modo trasparente, leale e dinamico sui trattamenti effettuati sui suoi dati (art. 13);
- il diritto di essere informato sulle violazioni dei propri dati personali entro 72 ore dall'evento (art. 33);
- il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente

[204] ALOVISIO, *Nuovo regolamento privacy UE: ecco tutto ciò che i cittadini e PA devono sapere*, in Agenda Digitale, 27 maggio 2016, reperibile *on-line*.
[205] *Ibidem*.
[206] Regolamento del 27 aprile 2016, n. 679 del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, art. 17: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) [...]".

costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per loro conto e di esercitare per loro conto i diritti sui propri dati (art. 80);
- il diritto di ottenere il risarcimento dei danni causato dalla violazione del regolamento (sancito sempre dall'art. 80 dello stesso).

È evidente che il regolamento comporti anche un cambiamento dal punto di vista culturale: viene modificato l'approccio fino ad ora utilizzato nei confronti del diritto alla *privacy*: difendere i dati significa oggi difendere le persone, l'identità e la libertà delle stesse. Inoltre, mediante tali atti si sta tentando di andare oltre le semplici regole formali affinché le norme a protezione dei dati vengano adeguate progressivamente ai cambiamenti determinati dall'incessante processo di evoluzione delle nuove tecnologie.
Adesso imprese e pubbliche amministrazioni, prima di procedere al trattamento dei dati personali, hanno l'obbligo di effettuare una valutazione (nota come *privacy impact assessment*) dei rischi connessi ad esso già nel momento della progettazione di nuove procedure, prodotti o servizi[207].
Un'altra novità introdotta dal regolamento riguarda la sua applicabilità: esso si rivolge a tutte le imprese, organizzazioni o enti che operano nell'ambito del trattamento dei dati personali all'interno dell'Unione europea, a prescindere dall'esatto luogo nel quale sono localizzati. Inoltre, essa trova applicazione nei confronti delle imprese che trattano dati personali sia nel caso in cui 'Titolare del trattamento' e 'Responsabile del trattamento' si trovino in uno Stato membro senza tener conto del fatto che il trattamento di dati personali avvenga all'interno dell'Unione o in un Paese terzo, sia nel caso in cui entrambi i soggetti non si trovino all'interno di uno Stato membro purché le attività dell'impresa in questione riguarda la fornitura di beni o servizi a cittadini dell'Unione europea o con il monitoraggio dei comportamenti di consumo all'interno della stessa.
Un altro aspetto di notevole importanza, derivante dalle disposizioni europee, riguarderà l'introduzione anche negli ordinamenti nazionali dei diversi Stati membri del c.d. 'principio di *accountability*' o obbligo di rendicontazione, in base al quale i titolari del trattamento dei dati devono dimostrare:

- di avere adottato le misure di sicurezza adeguate ed efficaci a protezione dei dati;
- che i trattamenti siano conformi con i principi e le disposizioni del regolamento europeo.

[207] ALOVISIO, *Nuovo regolamento privacy UE: ecco tutto ciò che i cittadini e PA devono sapere*, in *Agenda Digitale*, 27 maggio 2016, reperibile *on-line*.

Mediante l'art. 37, infine, viene istituita la nuova figura del '*Data Protection Officer*' (il responsabile della protezione dei dati personali), che deve essere nominato da ogni amministrazione pubblica al suo interno e da ogni azienda privata che svolge trattamenti sui dati potenzialmente in grado di ledere gravemente i diritti degli interessati.
Il *Data Protection Officer* (DPO) dovrebbe, secondo gli esperti, corrispondere ad un professionista esterno all'azienda in possesso di specifici requisiti quali la competenza (giuridica innanzitutto e informatica poi per poter interpretare correttamente le norme da applicare e per potersi rapportare adeguatamente con i responsabili dei sistemi informativi), l'esperienza, l'indipendenza e l'autonomia di risorse, l'assenza di conflitti di interesse; la sua persona dovrebbe, inoltre, avere anche le adeguate capacità per realizzare una completa analisi dei rischi connessi al trattamento dei dati e per valutare le interazioni con le altre discipline che riguardano, anche indirettamente, la sicurezza e la gestione delle informazioni[208]. Tutto ciò al fine di assolvere ai suoi compiti, fra i quali presidiare i profili *privacy* organizzativi attraverso un'opera di sorveglianza sulla corretta applicazione del regolamento europeo, della normativa *privacy* e sulla normativa interna, sull'attribuzione delle responsabilità, informazione, sensibilizzazione e formazione del personale, informazione, consulenza e rilascio di pareri.
Il *Data Protection Officer* costituisce, quindi, un punto di riferimento e di contatto per i cittadini al quale possono rivolgersi per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal regolamento europeo.
Il testo prevede, inoltre, un rafforzamento dei poteri delle Autorità garanti nazionali e un inasprimento delle sanzioni amministrative a carico di imprese e pubbliche amministrazioni: nel caso di violazioni dei principi e disposizioni del regolamento, le sanzioni possono arrivare, per le imprese, fino al 2-4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore; per le pubbliche amministrazioni fino a 10 milioni di euro.

Nei due anni di transizione verso l'applicazione del nuovo regolamento *privacy*, il Garante per la protezione dei dati personali svolgerà un ruolo chiave nella complessa opera di armonizzazione delle normativa nazionale in materia di protezione dei dati personali rispetto ai nuovi principi istituti nonché rispetto alle nuove responsabilità cui dovranno far fronte aziende, organizzazioni e pubbliche amministrazioni, previsti dal nuovo testo che punta a rafforzare la fiducia, la certezza legale e la concorrenza nell'ottica di costruire un nuovo dialogo con i cittadini e sviluppare un mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e *software*[209].

[208] RUSCONI, *Data Protection Officer: una figura strategica tra privacy e security*, 7 aprile 2017, ne *Il Sole 24Ore*, reperibile *on-line*.
[209] ALOVISIO, *Nuovo regolamento privacy UE: ecco tutto ciò che i cittadini e PA devono sapere*, in *Agenda Digitale*, 27 maggio 2016, reperibile *on-line*.

Il caso 'WannaCry': cosa sarebbe accaduto se il regolamento (UE) 2016/679 fosse stato già in vigore

Il 12 maggio 2017 è una data molto difficile per il mondo dell'informatica a causa della diffusione massiccia di un *ransomware*[210], noto come '*WannaCry*', che ha messo in ginocchio migliaia di computer colpendo circa 70 Paesi (tra cui l'Italia).

L'attacco non aveva un obiettivo preciso vero e proprio e i suoi autori hanno semplicemente bloccato in maniera diffusa i computer mediante un metodo molto semplice: l'invio di mail contenenti un *malware* in grado di prendere possesso di parte o di tutto il computer e di chiedere all'utente un riscatto (da pagarsi solitamente in '*bitcoin*'[211]) al fine di ottenere una chiave che permetta la restituzione del controllo sul proprio dispositivo, pena la perdita di tutti i dati ivi contenuti.

WannaCry è riuscito a diffondersi in tal modo sfruttando alcuni bug di Microsoft che già erano noti alla compagnia: di fatto, l'errore che ha aperto la strada al *ransomware* è consistito nella mancata attuazione dei necessari aggiornamenti dei computer colpiti, che si sono rivelati un 'terreno' molto fertile. Ecco perché è sempre più importante adottare misure di prevenzione oltre che di repressione rispetto ad eventuali attacchi informatici.

Nonostante il panico che ha generato, sembra che alla fine le aziende e le organizzazioni in tutto il mondo siano riuscite a fermare *WannaCry*, ma non è ancora il momento di sentirsi al sicuro: sembra, infatti, che si stia preparando un attacco ancor più grande di questo. Appare quanto mai necessario, allora, intervenire per proteggersi da eventuali futuri furti o alterazioni di dati.

In questo contesto, si inserisce la tutela garantita dal regolamento europeo del 27 aprile 2016, n. 679, che porterà le aziende ad operare una seria revisione delle loro strategie in ambito di *cyber security* e *data processing*.

Esso, infatti, stabilisce innanzitutto cosa si intende per violazione dei dati personali in modo da chiarire se e quando le aziende vittima di un attacco informatico come è stato *WannaCry*, che apparentemente non hanno visto i dati in loro possesso rubati ma solo criptati, possono incorrere in sanzioni per mancato adempimento delle clausole previste dallo stesso.

---

[210] Letteralmente 'virus del riscatto', il termine *ransomware* fa riferimento ad una vasta tipologia di virus in grado di bloccare il funzionamento di un computer facendo sì che l'utente non riesca a effettuare il login nel suo profilo utente o utilizzando la crittografia per rendere illeggibili i file presenti all'interno del disco rigido.

[211] Il *bitcoin* è una moneta elettronica creata nel 2009 da un anonimo inventore, noto con lo pseudonimo di Satoshi Nakamoto, che sviluppò un'idea da lui stesso presentata su Internet a fine 2008. A differenza della maggior parte delle valute tradizionali, il *bitcoin* non fa uso di un ente centrale: esso utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni e sfrutta la crittografia per gestire gli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione della proprietà dei *bitcoin.* Tale valuta è accettata come pagamento da un gran numero di commercianti come ogni altra valuta.
BUSTILLOS, *The Bitcoin Boom*, 1 aprile 2013, in *The New Yorker*, reperibile *on-line*.

Esaminiamo, innanzitutto, l'art. 4, par. 12, il quale afferma che per violazione dei dati personali si intende

> a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[212].

Nel caso di *WannaCry*, i dati dei clienti delle aziende o enti colpiti sono stati senza ombra di dubbio oggetto di un accesso illegale e sottoposti al rischio di perdita o alterazione.
In modo simile, l'art. 5, par, 1 precisa che i dati personali dovrebbero essere "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness andtransparency'), vale a dire che deve essere assicurata una loro protezione contro l'elaborazione non autorizzata o illegale e contro perdite, distruzioni o danni accidentali adottando le adeguate misure tecniche o organizzative per assicurare un livello di sicurezza appropriato[213]. A tal proposito, per valutare l'adeguato livello di sicurezza l'art. 32, par. 2, specifica che

> in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Dunque, se tale regolamento fosse già entrato in vigore molte aziende, non provvedendo ad attuare le adeguate misure di protezione che avrebbero sopperito alle vulnerabilità dei sistemi Windows-Microsoft, sarebbero state colpevoli, in altre parole, di aver permesso il trattamento non autorizzato o illegale dei dati dei clienti[214].
Questa vicenda mette, allora, in luce l'importanza di tale regolamento, elaborato per raggiungere uno scopo preciso: assicurare la protezione dei dati personali e, al contempo, una maggiore sicurezza rispetto al sopravvenire di un attacco informatico.

La direttiva 2016/680

Tale direttiva è rimasta quasi nell'ombra a causa della straordinaria popolarità, anche mediatica[215], del Regolamento 679/2016 destinato a ridisegnare la disciplina europea sulla *privacy* e a renderla, per la prima

[212] Regolamento del Parlamento europeo e del Consiglio del 27 aprile 2016, n. 679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
[213] *Ibidem.*
[214] DESTRI, *Cosa sarebbe successo se WannaCry fosse avvenuto dopo il GDPR*, 27 giugno 2017, CIO Business Technology Leadership, reperibile *on-line*.
[215] SCORZA, *Giustizia digitale Condivisione dati a fini giudiziari, ecco le nuove norme Ue*, in *Forumpa*, 23 maggio 2016, reperibile *on-line*.

volta, davvero uniforme; ciò nonostante essa non è da ritenersi affatto trascurabile. Tale direttiva si prefigge, infatti, lo scopo di disciplinare le regole concernenti la protezione delle persone con particolare riguardo verso il trattamento dei dati personali, andando quindi a completare quanto stabilito dal regolamento visto in precedenza. A sottolineare tale ruolo vi è lo stesso art. 1 della direttiva nel quale si afferma che essa:

> [...] lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

A fronte di ciò, gli Stati devono (e di fatto dovranno a partire dal 2018, data in cui entrambi gli atti entreranno in vigore) adempiere ad alcuni obblighi. In particolare, essi dovranno:

a) tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali;
b) garantire che lo scambio dei dati personali da parte delle autorità competenti all'interno dell'Unione, qualora tale scambio sia richiesto dal diritto dell'Unione o da quello dello Stato membro, non sia limitato né vietato per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali[216].

Attraverso tale direttiva, l'Unione europea, grazie ad un corretto trattamento dei dati personali, persegue principalmente due obiettivi: ridurre la loro esposizione ai rischi provenienti dal *cyber space* e aumentare la capacità degli Stati di proteggere gli stessi oltre che le reti informatiche.

In conclusione, l'Unione europea si propone di superare quel dilemma di cui molti esperti parlano, in base al quale in nome di un bene considerato superiore (la sicurezza) si possa limitare notevolmente la tutela di alcuni diritti e libertà fondamentali, e lo fa adottando un approccio che concilia il rafforzamento della sicurezza con la salvaguardia dei diritti umani.
A prova di ciò, vi sono anche le numerose risoluzioni del Parlamento europeo, che si è espresso su questioni delicate come il trattamento dei dati personali trasferiti nel quadro della cooperazione transatlantica nella lotta al terrorismo e alla criminalità organizzata, con l'obiettivo rendere nota questa nuova strada intrapresa dall'Unione[217]. Questi inoltre, sarà coinvolto anche nell'approvazione di un accordo quadro giuridicamente vincolante con gli Stati Uniti che è, a tal proposito, emblematico. Esso riguarda lo scambio di

[216] Direttiva del Parlamento europeo e del Consiglio del 27 aprile 2916, n. 680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, art. 1.
[217] MILT, *Protezione dei dati personali*, Parlamento europeo, 2017, reperibile *on-line*.

informazioni e dati relativi a individui che si sospetta possano essere coinvolti in atti terroristici o nella criminalità organizzata e prevede anche l'istituzione di uno Scudo UE-USA per la *privacy* ('*EU-US Privacy Shield*')[218], al fine di garantire un livello elevato di protezione dei dati che verranno scambiati al fine di cooperare nella lotta al terrorismo e alla criminalità organizzata. Dunque, da un lato si punta ad un rafforzamento della sicurezza nazionale, mediante efficaci politiche di *information sharing* che, allo stesso tempo, devono rispondere comunque alle norme in materia di diritti umani e, nello specifico, di protezione dei dati personali.
Al suo interno, viene delineata una serie di condizioni da soddisfare in materia di *privacy* e protezione dei dati personali che vengono scambiati tra i Paesi con l'obiettivo di monitorare gli individui sospettati di minacciare la sicurezza di Unione europea e Stati Uniti riuscendo così a salvaguardare anche i diritti umani degli individui in questione, *in primis* il diritto alla riservatezza.
L'approccio dell'Unione europea sembra percorrere, dunque, una via che persegue un costante equilibrio tra il rafforzamento della sicurezza, *in primis* delle reti informatiche, e la protezione della *privacy* e dei dati personali.
Questa è la strada che si dovrebbe continuare a percorrere al fine di elaborare efficienti politiche di *cyber security* che non compromettano la tutela dei diritti umani, il cui percorso evolutivo non può certo arrestarsi di fronte alle nuove sfide poste dal *cyber* spazio.

[218] *Ibidem.*

Conclusione

I sistemi informativi sono divenuti oggi vitali nella gestione di infrastrutture, dati personali, attività commerciali, enti amministrativi e via dicendo. Tuttavia, il *cyber space* è un mondo esposto a numerosi rischi, in quanto ricco di vulnerabilità (alcune delle quali sono ancora da scoprire). Dunque, muovendoci al suo interno, dobbiamo rimanere costantemente in uno stato di allerta tale da reagire a tutte quelle potenziali minacce che lo rendono un 'posto' meno sicuro. Infatti, le diverse vulnerabilità che caratterizzano i sistemi informativi, inizialmente creati senza pensare alle questioni legate alla sicurezza, possono essere sfruttate da un *hacker* per entrarvi illecitamente e leggere, trafugare, cancellare informazioni critiche e dati sensibili o addirittura prendere il controllo degli *assets* informatici o degli *assets* fisici a seconda dell'obiettivo che si persegue.
Negli ultimi anni, è cresciuto in maniera esponenziale il numero di attacchi informatici verificatesi, i quali sono sempre più complessi da identificare e prevenire e con effetti progressivamente più ampi (in termini di numero di Paesi colpiti e gravità dei danni arrecati).
La *cyber security* ha assunto, perciò, un ruolo fondamentale all'interno degli Stati, che cercano di aumentare le proprie difese ogni giorno anche mediante la diffusione di una cultura della sicurezza informatica, di una maggiore consapevolezza dei propri cittadini circa i rischi legati alle attività in rete e attraverso l'elaborazione di politiche di sicurezza più mirate.
Ad ogni modo, tali minacce non possono essere affrontate soltanto a livello nazionale: è necessaria una cooperazione a livello internazionale, innanzitutto per rafforzare la fiducia degli Stati e ridurre il rischio di conflitti (nei quali oggi giorno vengono impiegati anche i sistemi informativi); in secondo luogo, per permettere un'armonizzazione delle norme relative al perseguimento dei criminali informatici e la definizione di un quadro normativo più chiaro, perseguibile mediante la conclusione di trattati internazionali *ad hoc* o l'adattamento delle norme internazionali esistenti all'ambito delle *cyber operations*.
Alcune organizzazioni internazionali, fra le quali l'Osce, hanno già iniziato a muoversi in questa direzione.
Gli Stati partecipanti dell'Organizzazione per la Sicurezza e la Cooperazione in Europa hanno, infatti, deciso di elaborare delle misure di rafforzamento della fiducia (cosiddette CBM, '*Confidence building measures'*) per ridurre il rischio di conflitti derivanti dall'uso delle tecnologie dell'informazione e della comunicazione. Tali misure preventive mirano a rendere più prevedibile lo spazio cibernetico e offrono strumenti e meccanismi utili ad evitare possibili incomprensioni, quali:

- un meccanismo di consultazione tra gli Stati in caso di potenziali incidenti alla sicurezza informatica e cibernetica al fine di attenuare l'insorgenza di tensioni;
- una piattaforma per lo scambio di opinioni e di politiche ed approcci nazionali alla sicurezza cibernetica ed informatica al fine di permettere di 'leggere' meglio le intenzioni gli uni degli altri nel ciberspazio; e
- iniziative concrete per proteggere ad esempio infrastrutture informatiche sensibili al fine di permettere a tutti gli Stati partecipanti di rafforzare collegialmente la resilienza cibernetica nella regione dell'Osce a vantaggio di tutti[219].

Oltre all'attuazione di tali misure, per garantire la sicurezza cibernetica ed informatica, l'Osce e le sue istituzioni si occupano anche delle minacce alla sicurezza cibernetica ed informatica provenienti da attori non statali, quali criminalità organizzata e gruppi terroristici.
Si ritiene, infatti, che sia di importanza fondamentale, in questo ambito, spingere le autorità nazionali a reagire tempestivamente e in maniera adeguata a queste minacce, che sono in continua evoluzione, attraverso migliori tecniche forensi ed approcci innovativi; da qui, l'idea di elaborare linee guida comuni.
Anche durante le riunioni del G7, tenutesi nell'aprile del 2017 a Lucca, si è posto l'accento sulla necessità di collaborare per difendersi dagli attacchi informatici provenienti da attori statali e non.
Nella Dichiarazione sul *cyber* spazio, promossa dall'Italia e adottata durante le riunioni, è stato affermato dai diversi Ministri partecipanti quanto segue:

> ci impegniamo a mantenere il *cyber* spazio sicuro, aperto, accessibile, affidabile e interoperabili […] e riconosciamo il fatto che ogni Stato possa rispondere, in determinate circostanze, con contromisure proporzionate che prevedano anche l'uso di strumenti informatici come riconosciuto […] nella Carta delle Nazioni Unite[220].

Inoltre, in essa si espone il timore legato al rischio di

> […] escalation e ritorsioni nel *cyber* spazio, compresi massicci attacchi di tipo denial-of-service, danni alle infrastrutture critiche, o altre attività *cyber* dannose che compromettano l'uso e il funzionamento di un'infrastruttura critica che fornisce servizi al pubblico. Tali attività potrebbero avere un effetto destabilizzante sulla pace e la sicurezza internazionale[221].

[219] Decisione del Consiglio permanente dell'Osce del 20 marzo 2016, n. 1202, *misure Osce per il rafforzamento della fiducia volte a ridurre i rischi di conflitto derivanti dall'uso di tecnologie informatiche e di comunicazione.*
[220] Dichiarazione sul comportamento responsabile degli Stati nel cyberspazio, Lucca, 10-11 aprile 2017.
[221] *Ibidem.*

I Ministri degli Affari esteri degli Stati partecipanti hanno mostrato particolare preoccupazione per il tema, soprattutto in seguito ai numerosi attacchi avvenuti di recente (di cui abbiamo discusso nelle pagine precedenti).
Inoltre, mediante l'adozione di tale Dichiarazione gli Stati si impegnano a lavorare nell'ambito del G7 e altri pertinenti sedi internazionali e *multi-stakeholder*, per promuovere quadri strategici per la prevenzione di conflitti, la cooperazione e la stabilità nel *cyber* spazio.
Come possiamo osservare da quanto scritto nella Dichiarazione del G7 l'attenzione è rivolta soprattutto ai rischi legati alle attività di *cyber war* e al dovere degli Stati di assicurare non soltanto la sicurezza dei sistemi informativi ma anche il loro libero accesso. Si palesa, così, l'attenzione per la tutela dei diritti e delle libertà fondamentali accanto alla necessità di attuare politiche di sicurezza nazionale ed informatica.
Dunque, lo sguardo è rivolto contemporaneamente alle esigenze legate alla sicurezza dei sistemi informatici e alle istanze legate alla tutela dei diritti umani senza che un fattore escluda l'altro.
Con l'auspicio che si prosegua su questa via, possiamo concludere che, nonostante il cammino sia ancora lungo, gli Stati appaiono interessati ad intervenire (pur con le loro divergenze) nell'ottica di salvaguardare lo spazio virtuale.

Bibliografia

ALOVISIO (2016), *Nuovo regolamento privacy UE: ecco tutto ciò che i cittadini e PA devono sapere,* in *Agenda Digitale,* reperibile *on-line.*

AJAYI (2016), *Challenges to enforcement of cyber-crimes laws and policy,* in *Journal of Internet and Information Systems,* Nairobi, reperibile *on-line*.

ANTOLIN-JENKINS (2005), *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, in *Naval Law Review,* Volume 51, p. 132 ss.

ARCANGELI (2015), *Ixp e privacy delle telecomunicazioni*, in *GNOSIS 3/2015*, p. 117 ss.

ARKIN (1999), *The Cyber Bomb in Yugoslavia*, in *The Washington Post*, reperibile *on-line*.

BALDONI (2015), *Il futuro della cyber security in Italia*, CINL, Lucca.

BECK, HÜSER (2013) *Explanations for the Arab Spring*, Syddansk University.

BERNARD (2014), *Ways to Protect Yourself After the JPMorgan Hacking*, in *The New York Times*, reperibile *on-line*.

BUCHAN, ROSCINI, TSAGOURIAS (2014), *State Responsibility for Cyber Operations: International Law Issues*, *BRITISH Institute of International and Comparative Law*, reperibile *on-line*.

BUSTILLOS (2013), *The Bitcoin Boom,* in *The New Yorker,* reperibile *on-line*.

CALIFANO (2013), *Privacy e Sicurezza*, in *Democrazia e Sicurezza*, reperibile *on-line*.

CENCETTI (2014), *Cybersecurity: Unione europea e Italia, prospettive a confronto,* in *Quaderni IAI*, Roma, I ed.

CLARKE, KNAKE (2012) *Cyber War: The Next Threat to National Security and What to Do About It*, New York.

DESTRI (2017), *Cosa sarebbe successo se WannaCry fosse avvenuto dopo il GDPR,* CIO Business Technology Leadership, reperibile *on-line.*

DINNISS (2012), *Cyber Warfare and the Laws of War*, in *Cambridge studies in international and comparative law*, p. 4 ss.

EADS (2014), *China's Newest Export: Internet Censorship*, in *USNews*, reperibile *on-line*.

EVEN, SIMAN-TOV (2012), *Cyber Warfare: Concepts and Strategic Trends*, Tel Aviv, Memorandum n. 117.

FIDLER, PREGENT, VANDURME (2013), NATO, *Cyber Defense, and International Law*, Indiana University, reperibile *on-line*.

FORTSON (2016), *Cyber Security and the Need for International Governance*, in *National Law Review*, reperibile *on-line*.

GAZZELLA (2017), *La Corte Europea dei Diritti dell'Uomo riconosce la violazione della privacy del dipendente nei monitoraggi delle comunicazioni elettroniche effettuati per l'esercizio del potere disciplinare*, ne *Il Sole 24Ore*, reperibile *on-line*.

GOLDSTEIN, PERLROTH, SANGER (2014), *Hackers' Attack Cracked 10 Financial Firms in Major Assault*, in *The New York Times*, reperibile *on-line*.

GRECO (2014), *Cyber war e cyber security. Diritto internazionale dei conflitti informatici, contesto strategico, strumenti di prevenzione e contrasto*, in *Sistema Informativo a schede*, Archivio Disarmo, p. 3 ss.

GREEN, ROSSINI (2015), *Cyber Security and Human Rights*, in *Public Knowledge*, reperibile *on-line*.

HANDLER (2012), *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, in *Stanford Journal of International Law*, reperibile *on-line*.

HATHAWAY, CROOTOF, LEVITZ, NIX, NOWLAN, PERDUE, SPIEGEL (2012), *The Law of Cyber-Attack*, in *California Law Review*, p. 819 ss.

HERSCH (1952) *Oppenheim's International Law*, Londra, VII ed.

KUSHNER (2013), *The real story of Stuxnet*, IEEE Spectrum, vol. 50, Issue 3, reperibile *on-line*.

KULESZA, BALLESTE (2015) *Cybersecurity and Human Rights in the Age of Cyberveillance*, New York.

LIBICKI (1995) *What is Information Warfare?*, Washington, I ed.

LEE (2013), *Here's how Iran censors the Internet*, in *The Washington Post*, 15 agosto 2013, reperibile *on-line*.

MILT (2017), *Protezione dei dati personali*, Parlamento europeo, reperibile *on-line*.

MUNOZ (2014), *JP Morgan hack exposed data of 83 million, among biggest breaches in history*, in *REUTERS*, reperibile *on-line*.

NAGOURNEY, LOVETT, PÉREZ-PEÑA (2015), *San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead*, in *The New York Times*, reperibile *on-line*.

NATIONAL RESEARCH COUNCIL (2010), *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*.

MELZER (2011), *Cyberwarfare and International Law*, in *Resources, Ideas For Peace and Security*, reperibile *on-line*.

PINESCHI (2012), *Diritti umani (protezione internazionale dei)*, in *Annali della Enciclopedia del diritto*, vol. V, Milano.

RASKA (2015) *Confronting cyber security challenges: Israel's evolving cyber defence strategy*, NTU Singapore.

RIFFAT (2016), *Legal Aspects of Privacy and Security: A Case-Study of Apple versus FBI Arguments*, in *SANS Institute InfoSec Reading Room*, reperibile *on-line*.

RONZITTI (2013) *Introduzione al Diritto Internazionale*, Torino, IV ed.

RUSCONI (2017), *Data Protection Officer: una figura strategica tra privacy e security*, ne *Il Sole 24Ore*, reperibile *on-line*.

SANGER (2012), *Obama Order Sped up Wave of Cyber attacks Against Iran*, in *The New York Times*, reperibile *on-line*.

SCORZA (2016), *Giustizia digitale Condivisione dati a fini giudiziari, ecco le nuove norme Ue*, in *Forumpa*, reperibile *on-line*.

SHACKELFORD (2010), *State responsibility for cyber attacks: competing standards for a growing problem*, Cambridge, reperibile *on-line*.

SCHMITT (2011), *Cyber Operations and the Jus Ad Bellum Revisited*, in *Villanova Law Review*, Volume 56, p. 569 ss.

SCHMITT (2013) *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge.

SEMINARA (2015), *Libertà di espressione e internet. Riflessioni sulla sentenza della Corte europea dei diritti dell'uomo Delfi AS c. Estonia*, in *KOREUROPA*, reperibile *on-line*.

SETTI (2017), *Diritto e Guerra cibernetica*, in *Sicurezza nazionale*, reperibile *on-line*.

SILBER, BHATT (2007), *Radicalization in the West: The Homegrown Threat*, New York.

SINGER, FRIEDMAN (2014), *Cybersecurity and Cyberwar: what everyone needs to know*, Oxford.

SORDINI (2013) *La libertà di espressione nell'era digitare: disciplina internazionale e problematiche*, ISPI, reperibile *on-line*.

TETI (2013) *Cyber intelligence e cyber espionage come cambiano i servizi di intelligence nell'era del cyber spazio*, in *GNOSIS 3/2013*, p. 95 ss.

VICARELLI (2017), *La direttiva NIS: il primo passo della strategia europea per la cyber security*, in *Diritto informatico*, reperibile *on-line*.

VILLANI (2015) *Dalla Dichiarazione universale alla Convenzione europea dei diritti dell'uomo*, Bari, II ed.

WEISSBRODT (2013) *Cyber Conflict, Cyber Crime and Cyber Espionage*, in *Minnesota Journal of International Law*, p. 347 ss.

ZACCARIA (2009), *La libertà d'espressione e giurisprudenza della Corte Europea dei Diritti dell'Uomo*, reperibile *on-line*.

Il *cyber space*: una nuova dimensione per la conflittualità e la tutela dei diritti umani

Il presente elaborato si propone di offrire una panoramica dei fenomeni attinenti il *cyber* spazio e delle problematiche ad essi connesse.
Il primo capitolo è stato dedicato all'illustrazione dei concetti di *cyber* spazio, *cyber security*, *cyber crime* e *cyber attack*. Inoltre, in esso sono state analizzate le politiche in ambito *cyber* attuate dall'Unione europea e dall'Italia al fine di comprendere come hanno agito i Paesi europei posti di fronte a nuove minacce e nuovi scenari, come quello cibernetico.
Il secondo capitolo analizza, invece, il concetto di *cyber war* con lo scopo di illustrare questo nuovo fenomeno, comprendere quali sono gli attori che entrano in gioco e quali le sue conseguenze e peculiarità.
In questa prospettiva sono state esaminate, inoltre, le norme di diritto internazionale che disciplinano l'uso della forza nella Comunità internazionale, al fine di stabilire se esse trovino applicazione anche nell'ambito di questa nuova sfera di conflittualità.
Infine, il terzo capitolo si occupa dell'analisi dei vigenti sistemi di protezione dei diritti umani e, in particolare, del diritto alla libertà di espressione e del diritto alla *privacy*. In tale contesto, sono state analizzate le posizioni di coloro che sostengono la tesi secondo cui una maggiore tutela dei diritti umani comporterebbe una minore capacità degli Stati di garantire sicurezza e di coloro che ritengono possibile, al contrario, pervenire ad un bilanciamento tra la necessità di tutelare i diritti umani e il bisogno di assicurare il perseguimento di efficaci politiche di sicurezza nazionale, dove un'esigenza è complementare per il raggiungimento dell'altra. Il terzo capitolo si conclude dimostrando che, in realtà, è proprio questo secondo approccio a fornire il giusto equilibrio necessario per una più valida politica di *cyber security*.
Sulla scia dei concetti introdotti nel primo capitolo, necessari per la comprensione di quanto trattato in seguito, la tesi si pone pertanto, quale obiettivo ultimo, quello di analizzare il contesto *cyber* da diverse prospettive: da quella individuata nel secondo capitolo relativo alla disciplina dei conflitti armati alla luce delle nuove dinamiche cibernetiche, a quella individuata nel terzo capitolo relativo alla tutela dei diritti umani nell'ambito di politiche di sicurezza nazionale ed informatica.
Infine, si è cercato di individuare le criticità che ostacolano il corretto sviluppo di una normativa chiara e pressoché universale che disciplini tanto la guerra cibernetica quanto le adeguate misure di protezione e prevenzione rispetto ad eventuali attacchi cibernetici, potenzialmente lesivi dei diritti e delle libertà fondamentali dell'uomo.

Convenzionalmente, per indicare l'ambiente nel quale avvengono le operazioni che fanno uso delle reti informatiche, si utilizza il termine *cyber space*, che fa riferimento ad uno spazio virtuale privo di confini fisici, di limiti geografici e di un'autorità centrale di governo, al quale si può accedere mediante dispositivi in grado di collegarsi ad una rete informatica, in qualsiasi parte del mondo ci troviamo.
Il *cyber* spazio non deve essere, perciò, considerato un mondo puramente virtuale poiché accedere ad una connessione richiede, comunque, la presenza di oggetti fisici (dispositivi come computer, telefoni cellulari o *tablet*). Inoltre, dietro a tali dispositivi vi sono degli individui che influenzano e plasmano questo mondo, che condividono informazioni e che, a loro volta, vengono 'formati' da esso e stimolati al progresso tecnologico. Il *cyber space* è da ritenersi, quindi, un mondo caratterizzato dal dinamismo e in continua trasformazione nel quale il *know-how* dell'uomo porta alla produzione di tecnologie via via più sofisticate, determinanti interconnessioni sempre più profonde tra le varie parti del globo.
A tal proposito, rileva il concetto di *Internet of Things* (IoT), che sta ad indicare, di fatto, la diffusione di oggetti di uso comune collegati alle reti informatiche, il cui ambito di applicazione risulta ad oggi essere molto vasto. Sebbene la produzione di dispositivi IoT abbia, spesso, facilitato la gestione di attività quotidiane, innumerevoli sono i rischi legati al loro impiego.
Il termine *cyber security* è, nell'era contemporanea, frequentemente utilizzato dagli ambienti militari, dai media, dalle imprese private per indicare proprio il bisogno di difendersi all'interno dell'immenso spazio cibernetico, che appare progressivamente più insidioso.
Non esiste al momento una definizione universalmente riconosciuta di tale termine, tuttavia le varie definizioni fornite dagli esperti condividono un'unica premessa: non vi è soltanto il bisogno di proteggersi da un generale pericolo ma anche la presenza di un avversario dal quale difendersi, seppur spesso non ben identificato. Tale premessa costituisce la ragione per cui possiamo parlare di questioni di *cyber security* solo e soltanto quando un'attività perpetrata da uno o più individui avviene mediante l'utilizzo di reti informatiche e minaccia la sicurezza di un Paese.
Per questa ragione, non è sufficiente un semplice malfunzionamento dei sistemi informativi di un Paese, delle sue infrastrutture, delle reti di calcolatori e/o dispositivi elettronici personali ma è necessaria la presenza di una o più persone che volontariamente alterino la sicurezza di tali sistemi.
Un'efficace strategia di *cyber security* richiede, allora, un'analisi delle minacce, delle vulnerabilità e dei rischi associati all'impiego di sistemi informatici nonché l'attuazione di adeguate e specifiche misure difensive.
Quando parliamo di misure di *cyber security* è bene ricordare che queste possono consistere tanto in misure di prevenzione, le quali agiscono riducendo la probabilità di realizzazione di una minaccia, quanto in misure di protezione, le quali agiscono riducendo la gravità del danno prodotto da un attacco o crimine informatico.

In materia, nel contesto europeo è stata sviluppata, a partire dagli anni Duemila, una politica sempre più mirata verso questo settore che trova la sua massima espressione nella cosiddetta 'direttiva NIS (*Network and Information Security*)', approvata dal Parlamento europeo e dal Consiglio il 6 luglio 2016, la quale prevede il miglioramento delle capacità in materia di *cyber security* dei singoli Stati dell'Unione europea grazie all'adozione di specifiche misure di sicurezza a carico dei settori interessati; l'aumento del livello di cooperazione tra gli Stati dell'Unione; l'obbligo per gli operatori di servizi essenziali e dei fornitori di servizi digitali di adottare un approccio basato sulla gestione dei rischi e sulla comunicazione ad un'apposita autorità (e, in ultima analisi, all'ENISA - *European Network and Information Security Agency*, istituita mediante il regolamento (CE) 460/2004 per assistere la Commissione europea e gli Stati membri nella loro missione di prevenzione e reazione ai problemi di *cyber security*) circa tutti gli incidenti di una certa entità che si possono verificare nel *cyber* spazio; la designazione da parte di ciascuno Stato membro di un'apposita autorità che funga da punto di contatto per gli scambi internazionali e la costituzione ad opera dell'Unione di un gruppo di cooperazione al quale parteciperanno tutti gli Stati membri, la Commissione e l'ENISA.

Un'altra iniziativa che merita di essere trattata ha visto la luce il 5 luglio 2016, momento in cui la Commissione ha adottato una comunicazione che stabilisce varie misure per affrontare la frammentazione del mercato della sicurezza informatica dell'UE, atte a rafforzare la resilienza dell'Europa in materia di sicurezza informatica e a favorire la promozione del settore della *cyber* sicurezza.

Tra le azioni programmate, sarà istituita una rete di gruppi di intervento per la sicurezza informatica in tutta l'Unione europea, con l'obiettivo di garantire una reazione rapida alle minacce e agli incidenti digitali. Sarà, inoltre, istituito il c.d. 'gruppo di cooperazione' tra gli Stati membri per sostenere e facilitare la cooperazione strategica e lo scambio di informazioni e per aumentare la fiducia, in particolare in diversi settori dell'economia, comprese la formazione e l'istruzione in materia di sicurezza informatica.

A livello nazionale, guardando all'Italia, vediamo che solo recentemente essa ha iniziato a prestare attenzione ai fenomeni attinenti il *cyber* spazio.

Il 2013 è stato l'anno di svolta: viene approvato dal Presidente del Consiglio dei ministri il decreto del 22 gennaio 2013 *recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale* mediante il quale, per la prima volta, viene definita l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali.

In esso, vengono sostanzialmente individuati gli organi e gli enti nazionali incaricati di gestire eventuali situazioni di emergenza che possono prodursi in seguito ad eventi malevoli verificatisi nel *cyber* spazio. Nello specifico, al Presidente del Consiglio viene assegnato il compito di elaborare un Quadro strategico nazionale per la sicurezza dello spazio cibernetico e un Piano nazionale per la protezione cibernetica e la sicurezza informatica, su proposta e delibera del Comitato interministeriale per la sicurezza della

Repubblica (CISR). Inoltre egli, sentito il CISR, impartisce le direttive a DIS, AISE e AISI, ossia alle tre componenti dei servizi intelligence nazionali.
Facendo seguito all'emanazione del decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*, l'Italia riorganizza l'architettura istituzionale nata nel 2013 rendendola più snella ed efficace mediante l'assegnazione di un ruolo ancor più decisivo al DIS.
Questo nuovo provvedimento rafforza anche il ruolo del CISR, riconduce il Nucleo sicurezza cibernetica (che era stato istituito sempre nel 2013 presso l'Ufficio del Consigliere militare del Presidente del Consiglio quale ente di raccordo tra le diversi componenti dell'architettura istituzionale deputata ad intervenire in materia di sicurezza informatica) all'interno del DIS con la funzione di assicurare una risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale, in raccordo con tutte le strutture dei Ministeri competenti in materia, e prevede una forte interazione tra il Dipartimento della funzione pubblica, il Ministero dello sviluppo economico, il Ministero dell'interno, il Ministero dell'economia e finanza, il Ministero della difesa e l'Agenzia per l'Italia Digitale (istituita nel 2012 con la funzione di coordinare le azioni in materia di innovazione per promuovere le *Information and communication technologies* a supporto delle Pubbliche Amministrazioni).
Infine, il decreto attribuisce al Direttore generale del DIS il compito di definire le linee di azione per incrementare il livello di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici sia privati, cercando anche di individuare ed eliminare eventuali vulnerabilità.

Definite le politiche dell'Unione Europea e quella italiana, proseguiamo nella trattazione entrando nel merito dei temi attinenti la *cyber security* e la tutela dei diritti umani.

Quando parliamo di *cyber security* è opportuno fare una precisazione che riguarda la distinzione tra i due concetti di *cyber crime* e *cyber attack*.
Il primo indica l'insieme delle azioni commesse in violazione della legislazione internazionale e nazionale (laddove presente) che implicano l'utilizzo di computer o reti informatiche; rientrano, solitamente, in tale categoria crimini quali contraffazione, frodi, acquisizione di dati riservati, estorsione *on-line*, pedopornografia.
Il secondo indica, invece, l'insieme di azioni perpetrate mediante l'utilizzo di computer e *networks*, finalizzate ad indebolire o neutralizzare i sistemi computerizzati oggetto di attacco.
La caratteristica principale di un *cyber attack* è quella di essere per l'appunto un attacco, ossia il prodotto di una condotta attiva, sia che si parli di offesa attiva sia che si parli di difesa.
La seconda caratteristica da tenere bene a mente riguarda il fine ultimo dell'attacco informatico, che permette di distinguerlo da un semplice crimine

informatico: causare una paralisi della vittima, dimostrarne pubblicamente la fragilità, disseminare terrore negli individui. Ogni azione aggressiva commessa sia da un attore statale sia da un attore non statale e diretta a colpire la sicurezza nazionale di un Paese perciò, deve ritenersi un attacco informatico. Viceversa, qualsiasi azione che non persegua tale scopo, pensiamo alle frodi *on-line* o alla pirateria informatica, non rientra in tale definizione.
Possiamo distinguere tra due macro categorie di attacchi informatici: 'attacchi sintattici', ossia attacchi diretti contro un preciso bersaglio, che puntano a neutralizzare o distruggere, effettuati infettando i sistemi informatici oggetto di attacco attraverso *software* malevoli quali *virus*, *worms* o *Trojan Horses* e 'attacchi semantici', che solitamente consistono nella disseminazione di informazioni inaccurate in un sistema informatico al fine di arrestare un computer o una rete per ostacolare il libero accesso agli utenti autorizzati oppure di impedire l'accesso ad informazioni reali e corrette.
Ad essere oggetto di attacchi informatici spesso sono soprattutto le cosiddette infrastrutture critiche di un Paese. Gas, elettricità, sistemi di difesa, servizi finanziari e molto altro oggi dipendono, nella gran parte dei casi, da computer connessi tra di loro e alla rete. Nell'ipotesi in cui queste siano oggetto di un attacco informatico, qualsiasi sia la sua entità, un Paese potrebbe trovarsi completamente paralizzato o veder minata la propria stabilità e la propria capacità di proteggere la sua popolazione.
In tale contesto, si inserisce il concetto di *cyber war* (guerra cibernetica), da intendersi come l'insieme delle condotte poste in essere nel *cyber* spazio per manipolare, sabotare, danneggiare o distruggere sistemi informatici e/o obiettivi civili e militari ad essi connessi, al fine specifico di causare effetti corrispondenti alla minaccia o all'uso della forza armata, prima e/o durante un conflitto che vede la partecipazione di uno o più soggetti di diritto internazionale.
Per guerra cibernetica, dunque, non si intende una specifica categoria di guerra disciplinata da regole proprie, bensì l'impiego di particolari strumenti tecnico-informatici durante una guerra di stampo tradizionale, così come definita dal Primo e dal Secondo Protocollo Aggiuntivo alle Convenzioni di Ginevra (il primo relativo ai conflitti armati internazionali, il secondo ai conflitti armati non internazionali).
Alla luce della disciplina normativa derivante, invece, dalla Carta delle Nazioni Unite ci si è chiesti se l'impiego di mezzi informatici contro uno Stato possa essere considerato una violazione dell'art. 2, par. 4 della stessa, che pone un divieto assoluto di minaccia o uso della forza nell'ambito delle relazioni internazionali.
Per rispondere a tale quesito occorre analizzare, innanzitutto, il contenuto della Carta e capire quanto questo possa adeguatamente applicarsi anche al contesto delle *cyber operations*.
Partiamo dapprima dal concetto di minaccia: esclusi alcuni casi evidenti, come la presenza di un *ultimatum*, non è semplice identificare cosa possa

costituire una minaccia. Anche la Corte internazionale di giustizia si è pronunciata in tal senso, escludendo peraltro che ricorra la minaccia di uso della forza nel caso in cui uno Stato metta a punto un notevole livello di armamenti: questo perché nel diritto internazionale consuetudinario non esistono delle regole che impongono agli Stati sovrani dei limiti di armamento.
Lo stesso vale nel caso in cui uno Stato, avente relazioni piuttosto tese con un altro, iniziasse aggressivamente a sviluppare la propria capacità di condurre operazioni informatiche potenzialmente dannose: la semplice acquisizione di tale capacità non costituirebbe una minaccia; qualora, invece, questo dichiarasse che questa sarà impiegata per fini bellici e contro lo Stato considerato ostile, allora esso violerebbe l'art. 2, par. 4 della Carta delle Nazioni Unite ponendo in essere una minaccia all'uso della forza.
Secondariamente, riflettiamo sul significato del termine 'forza': parliamo soltanto di forza armata? In quali termini?
Secondo un'interpretazione sistematica della Carta si tratterebbe di forza armata, come confermato anche dagli stessi lavori preparatori allo statuto delle Nazioni Unite, da intendersi però in maniera ampia in modo da comprendere tanto il suo utilizzo in maniera diretta quanto quello in via indiretta. In tal modo, così come è accaduto nel caso *Nicaragua c. Stati Uniti* dove la Corte internazionale di giustizia ha qualificato la fornitura di armi da parte degli Stati Uniti come un atto di ingerenza negli affari interni del Nicaragua che si poneva in violazione dell'art. 2 par, 4 (in quanto finalizzata a influenzare e condizionare l'andamento degli eventi all'interno di un altro Stato), potremmo qualificare ad esempio il rifornimento nei confronti di un gruppo organizzato di *malware* oppure il loro addestramento al fine di realizzare un attacco informatico come uso o minaccia della forza.
Se ciò accadesse, riprendendo sempre quanto si afferma nella Carta delle Nazioni Unite (specificamente all'art. 39), sarebbe possibile allora l'intervento del Consiglio di Sicurezza, che potrebbe fare raccomandazioni, cioè adottare atti giuridicamente non vincolanti, oppure decidere di approvare misure non implicanti l'uso della forza (ai sensi dell'art. 41 della Carta) o misure implicanti l'uso della forza (ai sensi dell'art. 42) al fine di ristabilire la pace e la sicurezza internazionali. Sebbene questo sino ad oggi non sia mai avvenuto, in via teorica nulla esclude che in futuro il Consiglio di sicurezza possa esercitare la propria autorità anche in caso di *computer network attacks*.
Altra questione rilevante è la qualificazione di un attacco informatico quale attacco armato, data l'eventualità, prevista dalla Carta, che uno Stato possa direttamente agire da sé in risposta ad un attacco armato, esercitando il diritto di legittima difesa *ex* art. 51.
Secondo alcuni esperti sarebbe possibile identificare ed equiparare un attacco informatico ad un attacco armato attraverso un'interpretazione estensiva della Carta delle Nazioni Unite.
Le vie seguite per giungere a tale affermazione sono principalmente due.

Una fa riferimento all'obiettivo dell'attacco: si ritiene che, qualora un attacco colpisca un'infrastruttura critica di uno Stato, esso possa essere considerato un attacco armato a priori, al di là degli effettivi danni prodotti.
L'altra fa riferimento, invece, alle conseguenze e agli effetti di un attacco e classifica armato un attacco solo se questo provoca la morte o il ferimento di un certo numero di vittime, la distruzione di certe aree o proprietà o di altri 'oggetti tangibili'. In base a ciò, per essere considerato attacco armato, un *cyber attack* dovrebbe produrre i medesimi effetti di una classica operazione militare e questo, ad oggi, non è ancora avvenuto. Ad ogni modo, non possiamo escludere che ciò possa verificarsi nel futuro, pertanto è bene che si lasci ancora aperta questa possibilità.
Ciò detto, al momento vi è l'idea di poter ritenere applicabili alcune norme internazionali riguardanti l'uso della forza nelle relazioni internazionali anche al contesto *cyber* e, tuttavia, quest'interpretazione non si è ancora consolidata.
Nondimeno, è possibile che gli Stati scelgano addirittura, in futuro, di seguire una strada diversa che potrebbe portare alla conclusione di un trattato internazionale *ad hoc* che provveda a fornire un'interpretazione delle norme internazionali già esistenti più conforme al contesto cibernetico e a disciplinare le modalità di condotta di un'eventuale *cyber war*, similmente a quanto è stato fatto sino ad ora nell'ambito dei conflitti armati di stampo tradizionale.
Nello specifico, le questioni rilevanti che tale trattato dovrà affrontare riguardano anzitutto il riconoscimento di un attacco informatico quale minaccia o uso della forza, di modo che il Consiglio di sicurezza abbia la possibilità, effettuate le dovute analisi del caso, di intervenire qualora si ritengano minacciate la sicurezza e la pace internazionali, nelle modalità già previste dalla Carta delle Nazioni Unite.
La seconda questione da affrontare riguarderà la definizione di attacco informatico quale attacco armato: si dovrà, dunque, chiarire quando questo possa essere considerato tale. A tal proposito, è necessario che gli Stati trovino un accordo circa i requisiti che permetterebbero di attribuire ad un *cyber attack* tale qualifica e le conseguenti modalità di risposta ad esso, consistenti anche in ulteriori operazioni informatiche.
Infine, qualora i membri della Comunità internazionale dovessero trovarsi d'accordo, si potrebbero definire nuove norme in materia affrontando questioni già trattate dal diritto internazionale umanitario. In tal caso, operando sempre un forte adattamento al contesto cibernetico, si potrebbero specificare i casi in cui un attacco informatico, che abbia causato gravi danni o persino vittime, sia da considerarsi un illecito internazionale. Ancorché sino ad oggi non si sia mai verificato alcun attacco informatico di tale portata, di fatto non possiamo escludere che tale ipotesi possa essere presa in considerazione in futuro e disciplinata da norme scritte.

Nell'ambito di una guerra cibernetica, potrebbe altresì essere utile rifarsi al regime di responsabilità internazionale, laddove si riesca a provare che effettivamente dietro ad un *cyber attack* vi sia uno Stato.
In merito, occorre dire che la procedura atta a stabilire se un attacco informatico sia riconducibile ad uno Stato non è semplice: essa consta di diverse fasi.
Innanzitutto, è necessario risalire alla fonte d'origine dell'attacco; in secondo luogo, identificare l'individuo o il gruppo di individui che hanno perpetrato l'attacco e, infine, individuare un collegamento tra l'ideatore dell'attacco e, eventualmente, uno Stato.
Tale processo si caratterizza per una simultanea presenza di elementi tecnici, politici e giuridici.
Per quanto riguarda gli aspetti tecnici, facciamo riferimento al processo di identificazione forense riguardante la fonte dell'attacco informatico, che può offrire una più o meno certa geo-localizzazione del dispositivo dal quale l'attacco ha avuto origine. In questo modo, si può risalire al luogo in cui si trovava, probabilmente, chi ha dato avvio all'attacco o quanto meno il dispositivo dal quale esso è partito. Tuttavia, tale procedura non permette l'identificazione del responsabile. Quest'obiettivo viene perseguito, invece, mediante una sempre più frequente collaborazione con i servizi di intelligence, la quale genera uno scambio con le autorità di tutte quelle informazioni che essi sono in grado di raccogliere ed analizzare col fine di tracciare un profilo dell'autore dell'attacco, scoprire le sue abilità e le sue intenzioni ed infine risalire ad eventuali legami con uno Stato o con altri enti. È in questo frangente che emerge l'aspetto per lo più politico del processo di imputabilità di un atto ad uno Stato.
Per ciò che concerne, invece, l'aspetto legale rilevano le norme di diritto internazionale in materia.
Partiamo dalla definizione di responsabilità internazionale. Per responsabilità internazionale si intendono quelle relazioni giuridiche che vengono ad esistere in conseguenza della commissione di un fatto illecito secondo le regole di diritto internazionale, come specificato nell'art. 1 del *Progetto di articoli sulla responsabilità internazionale dello Stato*, adottato dalla Commissione di Diritto Internazionale nel 2001 che recita: "Every internationally wrongful act of a State entails the international responsibility of that State".
Tali relazioni consistono, di norma, in un rapporto giuridico tra lo Stato autore dell'illecito e lo Stato leso.
Il primo ha l'obbligo di effettuare una riparazione; il secondo ha il diritto di pretenderla e di comminare una contromisura nei confronti dello Stato autore dell'illecito. Cosa si intende quindi per illecito internazionale?
Secondo l'art. 2 del Progetto, gli elementi distintivi di un illecito internazionale sono due:

- l'elemento oggettivo, che consiste nella condotta (omissiva o commissiva) contraria ad una norma di diritto internazionale; a

riguardo è importante sottolineare che non rileva la natura della norma violata.

- l'elemento soggettivo, vale a dire l'accertamento che tale condotta sia imputabile ad uno Stato.

Per quanto riguarda il secondo elemento diverse sono le ipotesi per cui una determinata azione o omissione è imputabile ad uno Stato.
In primo luogo, è imputabile ad uno Stato la condotta di un suo organo. In questo caso, si parla sia degli organi del potere esecutivo sia di quelli del potere legislativo e giudiziario.
Consideriamo l'ipotesi in cui un attacco informatico abbia origine da un'infrastruttura governativa; si tratta di un organo statale o che comunque agisce in nome di uno Stato, pertanto secondo il diritto internazionale qualsiasi azione da questi commessa è imputabile ad esso. Tuttavia, il fatto che l'attacco provenga da un'infrastruttura statale, sebbene attesti senza dubbio un legame con uno Stato, non è di per sé condizione sufficiente a dimostrare la sua responsabilità in merito al fatto illecito compiuto. Questo è vero poiché è possibile che la stessa infrastruttura sia stata già oggetto di un attacco da parte di *hackers* che, una volta acquistatone il controllo, hanno sferrato un ulteriore attacco puntando su un altro obiettivo. Peraltro, operazioni di questo tipo non si limitano alle infrastrutture presenti sul territorio di uno Stato ma possono riguardare anche le navi, i velivoli e i satelliti di un Paese. Occorre, dunque, sempre indagare sui fatti per accertare l'eventuale responsabilità di uno Stato anche laddove, secondo le regole internazionali, apparentemente la responsabilità conseguente la commissione di un atto illecito sembrerebbe molto semplice da attribuire ad esso.
Secondo la Corte internazionale di giustizia (in base alla cosiddetta teoria dell'*effective operational control*) sono equiparabili ad organi dello Stato anche le persone non dotate di tale qualifica nel diritto interno, purché si dimostri che lo Stato ritenuto responsabile eserciti su di esse un significativo grado di controllo che dia luogo ad una relazione di completa dipendenza tra l'agente e lo Stato.
Una diversa interpretazione della nozione di 'controllo' da parte di uno Stato su un gruppo di individui è stata fornita, invece, dal Tribunale Internazionale per la Jugoslavia: esso ha sancito il concetto di *'overall control*', espressione con la quale si vuole indicare l'insieme di atti mediante i quali uno Stato non soltanto supporta un gruppo di privati ma ne organizza e coordina le attività. Stiamo parlando, dunque, di un controllo più globale che non sottende però un rapporto di completa dipendenza dallo Stato stesso e questa è la grande differenza tra le due interpretazioni in merito. La Commissione di diritto internazionale ha rifiutato, invece, tale accezione optando per la teoria secondo cui il controllo deve essere effettivamente esercitato su ogni specifico atto lesivo.
Nel *Progetto di articoli* si afferma, inoltre, che si possono considerare organi statali le persone o gli enti comunque sprovvisti di tale qualità in base al

diritto interno dello Stato solo ove essi siano abilitati da questo ad esercitare prerogative dell'autorità di governo ed agiscano in tale qualità.
Al di là di queste ipotesi, normalmente la condotta di semplici individui non è imputabile ad uno Stato, a meno che la condotta di uno o più privati non venga fatta propria da questo, come è accaduto nel noto caso degli ostaggi a Teheran. Soltanto in tale circostanza, dunque, lo Stato risponde direttamente della condotta di un individuo. Da ciò ne discende che qualsiasi attività di *cyber warfare* intrapresa da privati, se fatta propria da uno Stato, è imputabile a quello Stato. Lo stesso vale per le agenzie private o governative che si comportano di fatto come organi dello Stato poiché agiscono su istruzione o sotto la direzione o il controllo di questo. Ricordiamo, però, che la dottrina sposa la tesi secondo cui il controllo dello Stato debba effettivamente essere esercitato su ogni atto lesivo.
Un'altra ipotesi prevede che, qualora un organo sia messo a disposizione di un altro Stato, la sua condotta lesiva sarà imputabile allo Stato a disposizione del quale è posto. In tal caso, pur trattandosi comunque di organo statale, come abbiamo già visto, non è così scontato che effettivamente uno Stato sia considerato il vero responsabile.
Infine, il diritto internazionale (sulla base di quanto accaduto nel caso del Canale di Corfù) stabilisce che uno Stato, consapevole del fatto che il suo territorio o le sue reti di informazione vengano utilizzati da un altro Stato o da un gruppo di attori privati per compiere attività illecite contro terzi, fra le quali rientrano quelle di *cyber warfare*, possa essere ritenuto responsabile della commissione di un illecito internazionale qualora non attui misure sufficienti a prevenire tali attacchi o non dia avviso di quanto sta accadendo. Nondimeno, potrebbero verificarsi circostanze tali per cui uno Stato possa non essere in grado di prevenire che un attacco venga lanciato o avvisare un altro Stato a causa della scarsità delle informazioni in suo possesso riguardanti la fonte d'origine dell'attacco, il momento esatto in cui esso sarà lanciato o il *target* di riferimento. In tal caso, spetterebbe ad un organo, quale ad esempio la Corte internazionale di giustizia, analizzare il susseguirsi degli eventi e stabilire se esistano o meno le condizioni per far scattare la responsabilità internazionale dello Stato in questione.
In conclusione, possiamo affermare che il diritto internazionale offre già un quadro normativo ipoteticamente applicabile al caso dei *cyber attacks*, quantomeno in relazione alla probabilità che un attacco, sia pur perpetrato da privati, sia imputabile ad uno Stato. Il problema è che non sempre risulta semplice individuare chi ha perpetrato l'attacco e soprattutto rinvenire poi un collegamento con uno Stato. Inoltre, data la trans-nazionalità che spesso caratterizza i *cyber attacks*, è sempre più difficile per uno Stato rivalersi su un altro.
Vale la pena comunque soffermarsi sulle conseguenze che si potrebbero avere una volta accertata tale responsabilità.
A quel punto, infatti, lo Stato leso può esercitare il proprio diritto di chiedere immediatamente una riparazione e di intraprendere delle contromisure, in risposta all'attacco subìto. Sembra al momento possibile rispondere ad un

attacco ricorrendo persino a contromisure in ambito *cyber* purché si rispettino però i requisiti stabiliti dal diritto internazionale a riguardo: tali contromisure dovranno:

- avere carattere pacifico, in modo da non violare l'art. 2 par, 4 della Carta ONU;
- rispettare il criterio della proporzionalità rispetto alla lesione subita, come stabilito dall'art. 49 del *Progetto di articoli* redatto dalla Commissione di diritto internazionale. Questo perché l''effetto della contromisura non deve essere manifestamente sproporzionato rispetto alla gravità dell'illecito internazionale commesso;
- rispettare le norme di *jus cogens* e di diritto umanitario.

Ad ogni modo, adottare contromisure significherebbe adottare un approccio di difesa attiva, che potrebbe ingenerare una *escalation* degli eventi; una migliore opzione potrebbe consistere nella realizzazione di strategie di difesa passiva, in grado di impedire o vanificare gli effetti di un attacco piuttosto che dovervi reagire.

Ciò detto, la difesa del *cyber* spazio non riguarda soltanto l'ambito militare bensì anche quello civile. Il mondo della *cyber security* è, infatti, sempre più legato sia alla nozione di sicurezza nazionale sia al tema della sicurezza dei dati e della tutela dei diritti umani in rete.
Internet è diventato, di fatto, uno dei mezzi di comunicazione più utilizzati nel mondo ed è l'unico che permette una globale e rapida diffusione di informazioni tale da offrire, al contempo, a coloro che vi operano sia la possibilità di attingere alle sue fonti sia quella di condividere i propri dati, anche sensibili e personali. Per questa ragione, e per la crescente frequenza di attacchi *cyber*, si è ravvisata l'importanza di promuovere il rispetto dei diritti umani, ed in particolare del diritto alla libertà di espressione e del diritto alla *privacy*, anche e soprattutto entro il contesto cibernetico.
Per quanto riguarda la libertà di espressione, si sente spesso parlare di '*Internet freedom*', un concetto che fa riferimento al diritto di accesso ad Internet come mezzo 'per' e 'al fine di' connettere gli individui a livello globale, messo a volte a repentaglio dalle stesse politiche di *security* intraprese dagli Stati oppure dalla commissione di attacchi informatici.
A titolo d'esempio analizziamo il caso dell'Estonia del 2007.
Il 27 aprile 2007 l'Estonia decise di rimuovere dalla capitale Tallin, e spostare verso un cimitero militare situato fuori dalla città, una statua di bronzo alta più di due metri raffigurante un soldato con l'uniforme dell'Armata Rossa, morto durante la II guerra mondiale in seguito ad uno scontro con i nazisti, diventata simbolo della sua vecchia appartenenza all'URSS.
A quest'evento seguirono numerose proteste da parte dei cittadini estoni di origine russa, che presto sfociarono nella violenza e nell'arresto di diverse persone. A ciò si aggiunse una serie di attacchi DDoS (Distributed Denial-

of-Service) contro numerosi siti web nazionali che furono resi inaccessibili; inoltre, si provocò la paralisi di tutte quelle sovrastrutture collegate alla rete (come il governo o le banche nazionali). La questione si risolse con l'intervento da parte della NATO e degli USA, i quali inviarono dei loro esperti nel Paese per investigare e proteggere i sistemi informatici da ulteriori minacce.
A livello internazionale, ma anche a livello regionale, esiste già comunque un regime di tutela dei diritti fondamentali, fra i quali rientra la libertà di espressione, che risulta del tutto applicabile al contesto *cyber* poiché, come sancisce la Dichiarazione universale dei diritti dell'uomo (la cui importanza storica, politica e giuridica è riconosciuta parimenti da tutti i membri della Comunità internazionale), tali diritti devono essere garantiti a prescindere dai confini territoriali di uno Stato e a prescindere dalle modalità o dagli strumenti attraverso i quali gli individui provvedono a ricercare, ricevere e condividere informazioni.
Questo è uno dei motivi per cui solitamente si prevedono restrizioni alla tutela di tali diritti soltanto in circostanze particolari, con la garanzia che siano sempre rispettati i principi di necessità e di proporzionalità rispetto all'interesse che si considera in quel momento preminente, seppur permanga l'idea di assicurare un bilanciamento fra i vari interessi in gioco.
Nel caso *Yildirim c. Turchia*, ad esempio, la Corte europea ha esplicitamente sostenuto che impedire l'accesso al sito ad una larga parte di popolazione aveva rappresentato un'interferenza del governo turco e una violazione dell'art. 10 della Convenzione, che tutela proprio la libertà di espressione.
In tale occasione, essa ha provveduto anche a precisare che eventuali misure restrittive devono essere previste per legge, devono costituire misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione di reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui e che occorre preventivamente verificare la possibilità di adottare dapprima misure meno severe.
L'importanza della tutela del diritto alla *privacy* all'interno del *cyber space* è stata, invece, rilevata soprattutto alla luce del fatto che in esso la diffusione di dati è incredibilmente semplice e veloce e, tuttavia, numerose sono le vulnerabilità dei sistemi informativi che rendono altrettanto facile la loro manipolazione o il loro furto.
Il diritto alla *privacy*, infatti, deve essere inteso non soltanto come diritto di non interferenza nella vita privata del singolo ma anche come diritto alla protezione di tutte quelle informazioni riguardanti tale sfera personale.
Oggigiorno, tuttavia, a fronte della necessità di proteggersi, si sta facendo strada l'idea che la *privacy* debba cedere il passo alla sicurezza e che, per garantire protezione ai propri cittadini, sia necessario apporre restrizioni ad alcuni diritti e libertà individuali fra i quali proprio questo.
Non appare del tutto impossibile percorrere, invece, un'altra strada.
In parte questa via è stata intrapresa dalla Corte europea dei diritti dell'uomo che, nel caso *Bărbulescu c. Romania*, ha tenuto a ribadire l'importanza di

garantire tanto la sicurezza, in questo caso di un'azienda (quella dove era impiegato il ricorrente, licenziato in seguito ad un'attività di monitoraggio dell'utilizzo del suo account lavorativo, ritenuto poco professionale) ma in generale degli Stati, quanto la *privacy* degli individui.
A virare in questa direzione è poi l'Unione europea mediante l'approvazione del 'General Data Protection Regulation'che, insieme alla direttiva (UE) 2016/680, costituisce il cosiddetto 'pacchetto protezione dati personali'.
Il testo di tale regolamento riconosce un livello elevato e uniforme di tutela dei dati personali e si pone come fine ultimo quello di offrire ai cittadini europei un maggiore controllo di questi ultimi.
Esso pone i cittadini e i loro diritti in primo piano e, in sintesi, riconosce loro:

- il diritto alla portabilità dei dati (art. 20), ossia il diritto a ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i propri dati personali forniti ad un titolare del trattamento e il diritto di trasmettere tali dati ad un altro titolare senza impedimenti;
- il diritto all'oblio, riconosciuto fino ad ora solo a livello giurisprudenziale, che prevede il diritto di ottenere dal titolare del trattamento la cancellazione dei propri dati personali senza ingiustificato trattamento se sussiste uno dei motivi elencati all'art. 17 del regolamento;
- il diritto di essere informato in modo trasparente, leale e dinamico sui trattamenti effettuati sui suoi dati (art. 13);
- il diritto di essere informato sulle violazioni dei propri dati personali entro 72 ore dall'evento (art. 33);
- il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per loro conto e di esercitare per loro conto i diritti sui propri dati (art. 80);
- il diritto di ottenere il risarcimento dei danni causato dalla violazione del regolamento (sancito sempre dall'art. 80 dello stesso).

Inoltre, tale regolamento sancisce l'obbligo per le imprese e le pubbliche amministrazioni, prima di procedere al trattamento dei dati personali, di effettuare una valutazione (nota come *privacy impact assessment*) dei rischi connessi a questo già nel momento della progettazione di nuove procedure, prodotti o servizi, e introduce negli ordinamenti nazionali dei diversi Stati membri dell'UE il c.d. 'obbligo di rendicontazione', in base al quale i titolari del trattamento dei dati devono dimostrare di avere adottato le misure di sicurezza previste dal regolamento.

Con l'art. 37, infine, viene istituita la nuova figura del '*Data Protection Officer*' (il responsabile della protezione dei dati personali), il quale presidia circa la sua corretta applicazione e svolge altresì opera di consulenza mediante la redazione di pareri.
Tale regolamento persegue, dunque, il duplice obiettivo di assicurare la protezione dei dati personali e al contempo maggiore sicurezza rispetto al sopravvenire di un attacco informatico grazie ad un corretto trattamento dei dati personali, che risultano così meno soggetti ai rischi provenienti dal *cyber space*.
La direttiva n. 680 completa la disciplina in materia di protezione dei dati personali ponendo a carico degli Stati diversi obblighi, fra i quali l'adozione di misure di tutela dei diritti e delle libertà fondamentali delle persone fisiche, in particolare del diritto alla protezione dei dati personali, e la garanzia che, qualora lo scambio di dati personali da parte delle autorità competenti all'interno dell'Unione sia richiesto dal diritto dell'Unione o da quello dello Stato membro, esso non risulti limitato né vietato per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
È evidente, dunque, che nel contesto europeo si è deciso di affrontare le minacce provenienti dallo spazio cibernetico mediante politiche di sicurezza più mirate, finalizzate a raggiungere una maggiore armonizzazione delle norme in materia, laddove esistenti, o a colmare il vuoto normativo che rendeva difficile il perseguimento di una valida politica di *cyber security*.
Nondimeno, si sta tentando di non trascurare la tutela dei diritti fondamentali che risultano oggi esposti, e presumibilmente lo saranno ancor di più in futuro, ad un'insidiosa minaccia proveniente dal mondo cibernetico. In materia, la recente disciplina dell'Unione europea sembra offrire un modello da imitare.
Con l'auspicio che si prosegua su questa via, possiamo concludere che, nonostante il cammino sia ancora lungo, gli Stati appaiono interessati ad intervenire (pur con le loro divergenze) nell'ottica di salvaguardare lo spazio virtuale.