LUISS

Corso Di Laurea in Giurisprudenza

Cattedra di Diritto Internazionale

# Cyberspionaggio: la Guerra Fredda del Ventunesimo Secolo


Prof. Roberto Virzo

RELATORE

Prof. Pietro Pustorino

CORRELATORE

Ludovica Liso

CANDIDATO

Matr.163873



Anno Accademico 2023/2024

## INDICE

# INTRODUZIONE

Negli ultimi decenni, lo sviluppo esponenziale delle tecnologie informatiche ha trasformato profondamente il modo in cui gli Stati interagiscono tra loro, sia in termini di cooperazione che di conflitto. In questo contesto, lo spionaggio informatico è emerso come una delle minacce più rilevanti per la sicurezza nazionale e internazionale, capace di influenzare gli equilibri geopolitici, la stabilità economica e la tutela della privacy individuale. Le informazioni digitali, diventate una risorsa strategica di primaria importanza, sono oggi al centro di un'intensa attività di raccolta e sfruttamento da parte di governi, organizzazioni e attori non statali.

L'obiettivo di questa tesi è analizzare lo spionaggio informatico attraverso una prospettiva giuridica e geopolitica, evidenziandone le implicazioni per il diritto internazionale e la sicurezza globale. Lo studio si articola in tre capitoli che, nel loro insieme, forniscono un quadro completo del fenomeno, dalle normative vigenti ai casi concreti, fino agli scenari futuri.

Nel Primo capitolo, viene trattato il quadro normativo nazionale e internazionale relativo allo spionaggio informatico. Il diritto internazionale, tradizionalmente incentrato sulla regolamentazione dei conflitti armati e sulle relazioni diplomatiche, si trova oggi di fronte a nuove sfide legate alla cybersicurezza. Sebbene esistano convenzioni e trattati che disciplinano la tutela delle informazioni e la protezione dei dati, la regolamentazione dello spionaggio informatico rimane frammentaria e spesso inadeguata a fronteggiare le moderne minacce digitali. Il capitolo analizza le principali disposizioni giuridiche in materia, esaminando sia le norme nazionali di alcuni Stati chiave, sia gli accordi internazionali esistenti, con particolare attenzione alle difficoltà di applicazione e di enforcement delle misure normative in un contesto transnazionale.

Il Secondo Capitolo si concentra su tre casi emblematici che hanno segnato la storia recente dello spionaggio informatico: il caso WikiLeaks, il caso Datagate e lo spionaggio informatico nel conflitto russo-ucraino. Il caso WikiLeaks ha messo in discussione il confine tra trasparenza e sicurezza nazionale, evidenziando come la divulgazione di documenti riservati possa avere profonde ripercussioni sulle relazioni diplomatiche internazionali. Il Datagate, reso noto dalle rivelazioni di Edward Snowden, ha sollevato interrogativi sulla sorveglianza di massa e sulla

tutela della privacy nell'era digitale, rivelando le pratiche di intelligence adottate dagli Stati Uniti nei confronti di cittadini e governi alleati. Infine, l'analisi del conflitto russo-ucraino offre uno spaccato delle nuove strategie di guerra ibrida, in cui le operazioni di cyberspionaggio svolgono un ruolo cruciale nel raccogliere informazioni strategiche, influenzare l'opinione pubblica e destabilizzare le infrastrutture critiche di un Paese.

Nel Terzo capitolo, l'attenzione si sposta sugli scenari futuri dello spionaggio informatico e sull'impatto delle nuove tecnologie, in particolare l'Intelligenza artificiale. Con l'evoluzione degli strumenti di attacco e difesa nel cyberspazio, l'IA sta assumendo un ruolo sempre più determinante nel migliorare le capacità di analisi, predizione e automazione delle operazioni di intelligence. Tuttavia, l'uso di sistemi basati sull'intelligenza artificiale solleva interrogativi etici e giuridici, soprattutto in termini di responsabilità, trasparenza e controllo degli algoritmi impiegati per il monitoraggio e la raccolta di dati sensibili. Il capitolo esplora i possibili sviluppi della cyber-intelligence e le implicazioni per la sicurezza globale, analizzando il ruolo degli Stati e delle organizzazioni internazionali nel definire un quadro normativo adeguato per prevenire abusi e garantire un equilibrio tra sicurezza e diritti fondamentali.

Attraverso l'analisi di questi aspetti, la tesi si propone di fornire una visione critica e aggiornata dello spionaggio informatico, mettendo in evidenza le sue implicazioni giuridiche, politiche e strategiche. L'evoluzione delle tecnologie digitali e la crescente interconnessione tra Stati rendono necessaria una riflessione approfondita sulle sfide poste dal cyberspionaggio e sulle possibili soluzioni normative e diplomatiche per affrontarle. In un mondo sempre più dipendente dai flussi informativi e dalle reti digitali, la capacità di bilanciare sicurezza, trasparenza e tutela dei diritti sarà cruciale per garantire la stabilità e la cooperazione internazionale.

# CAPITOLO I

# Normativa Nazionale e Internazionale

## 1 Definizione di spionaggio informatico

Homo homini lupus, tale proverbio che trae origine dall'Asinaria di Plauto, vuole alludere all'egoismo umano, e assunto dal filosofo T. Hobbes, nella sua opera *De cive*, per designare lo stato di natura in cui gli uomini, soggiogati dall'egoismo, si combattono l'un l'altro per sopravvivere. Questo concetto si inserisce perfettamente nel contesto della guerra, che rappresenta una delle espressioni più estreme della violenza e della competitività tra individui o stati. Come sottolineato da Hobbes nel suo "Leviatano", in uno stato di natura, senza un'autorità centrale che imponga le leggi, gli uomini vivono in uno Stato di "guerra di tutti contro tutti". Le guerre, specialmente quelle civili o che coinvolgono stati falliti, possono essere viste come il ritorno a questa condizione hobbesiana in cui prevalgono violenza e anarchia. Gli Stati, mossi da necessità geopolitiche, economiche o ideologiche, possono decidere di intraprendere guerre per assicurarsi risorse o rafforzare la propria supremazia, dimostrando come l'uomo sia pronto a sopraffare il proprio simile per il proprio tornaconto, proprio come descritto dal brocardo. Hobbes sosteneva che la paura della violenza altrui spingeva l'uomo a cercare la propria sicurezza attraverso la sottomissione a un'autorità forte o, in assenza di questa, attraverso il conflitto. Molte guerre, storicamente, sono iniziate proprio per ragioni di sicurezza, con gli stati che attaccano preventivamente o reagiscono a una percezione di minaccia, incarnando l'idea di "homo homini lupus". L'evoluzione della guerra ha sempre portato con sé una parallela trasformazione delle tecniche di spionaggio, che hanno avuto un ruolo cruciale nell'ottenere vantaggi strategici e tattici. Fin dalle epoche antiche, lo spionaggio è stato considerato uno strumento essenziale per la raccolta di informazioni su nemici o potenziali minacce, ma con il progredire della tecnologia e l'intensificarsi dei conflitti, le modalità e le finalità dello spionaggio si sono evolute in maniera significativa. Nei conflitti del passato, lo spionaggio si basava principalmente su agenti fisici infiltrati nei territori nemici, che raccoglievano informazioni tramite osservazione diretta, intercettazione di comunicazioni o tradimento. Le guerre

moderne, a partire dalle due guerre mondiali, hanno visto l'introduzione di tecnologie avanzate come la crittografia, la radio, il radar e gli aerei da ricognizione. Questi sviluppi hanno reso la raccolta di informazioni più sofisticata, ma anche più indispensabile, per l'identificazione di obiettivi, movimenti di truppe e la pianificazione strategica. Con l'avvento della Guerra Fredda, lo spionaggio ha subito un'accelerazione tecnologica senza precedenti. In questa fase, caratterizzata dalla contrapposizione tra Stati Uniti e Unione Sovietica, l'informazione è diventata l'arma principale. Le operazioni di spionaggio erano incentrate non solo sulla raccolta di dati militari, ma anche su informazioni politiche, economiche e scientifiche, essenziali per mantenere la superiorità strategica. In questo contesto è nato il cyberspionaggio, come risultato della crescente informatizzazione delle comunicazioni e delle infrastrutture. Il termine “spionaggio” evoca un periodo storico caratterizzato da forti tensioni internazionali, alimentate da profonde divergenze ideologiche che, in più di un'occasione, sfociarono in veri e propri conflitti militari protrattisi per anni. La “Guerra Fredda” è stata senza dubbio uno dei momenti in cui lo spionaggio ha giocato un ruolo centrale, con una continua lotta segreta tra il blocco occidentale e quello sovietico. Questo scontro, fatto di intrighi, omicidi, sottrazione di segreti, doppi giochi, scambi di spie e l’utilizzo di tecnologie di spionaggio incredibilmente avanzate per l’epoca, ha lasciato un’impronta indelebile nella storia. Tuttavia, la "guerra delle spie" non ha avuto solo ripercussioni politiche e militari, ma è stata anche una fonte inesauribile di ispirazione per giornalisti, scrittori e registi, che hanno dato vita ad alcune delle opere cinematografiche e letterarie più prolifiche e iconiche di tutti i tempi, un fenomeno che continua ancora oggi. Lo spionaggio – come anche il controspionaggio – è un’attività dell’intelligence finalizzata alla ricerca informativa di segreti o informazioni non di dominio pubblico, prevalentemente di avversari o nemici, onde poter ottenere vantaggi economici, sociali, politici e militari è un elemento fondamentale per la vita politica, sociale, economica e della sicurezza di uno Stato. L’attività di spionaggio e controspionaggio non si limita alle intelligence statali ma negli ultimi anni si sta radicando nel settore industriale soprattutto nelle aziende. Il mondo dello spionaggio appare senza limiti, barriere geografiche e temporali in funzione dell’utilizzo della rete Internet, può essere manipolata attraverso delle azioni di comunicazione finalizzate al condizionamento e alla persuasione.

L’avvento di nuove tecnologie ha segnato in maniera indelebile il volto del XXI secolo. Possiamo parlare di *Cyber war* una guerra che non è caratterizzata da bombe od armi bensì è articolata da più attacchi complessi senza limitazioni di alcun genere, finalizzati al trafugamento/disintegrazione delle informazioni contenute nei sistemi informativi di governi, aziende e organizzazioni diverse. All’utilizzo delle tecnologie si affianca il lavoro di professionisti specializzati in attività di intelligence. L’evoluzione del fenomeno del terrorismo internazionale, l’inarrestabile sviluppo delle *Cyber War* sono solo alcune delle tematiche che devono essere tenute costantemente sotto controllo dai servizi segreti. La nostra vita viaggia parallelamente al Cyberspazio, dunque, lo spionaggio cibernetico rappresenta il futuro delle attività di intelligence mondiali. [1] L'avvento di Internet e delle tecnologie digitali ha segnato l'inizio di una nuova era, in cui gli individui comuni non solo consumano informazioni, ma ne diventano attivi produttori. Questo cambiamento ha rivoluzionato i processi di ricerca, acquisizione e analisi dei dati, che oggi si basano su strumenti e metodologie completamente diversi rispetto al passato. Il cyberspazio è diventato il nuovo ambiente da cui attingere informazioni per le operazioni di intelligence. Di conseguenza, negli ultimi trent'anni, i servizi segreti hanno dovuto adattarsi a queste trasformazioni, dando vita a un'evoluzione significativa nelle tecniche e nelle modalità di spionaggio, che ora richiedono competenze altamente specializzate e un'ampia dotazione di strumenti tecnologici avanzati. Lo spionaggio, nell'immaginario collettivo, richiama scenari in cui agenti segreti si impegnano a raccogliere informazioni o a compiere azioni di sabotaggio per conto di governi o organizzazioni. Nella sua accezione tradizionale, è l’essere umano a giocare un ruolo centrale nello svelare segreti e recuperare informazioni. Tuttavia, nello spionaggio informatico, le operazioni si fondano principalmente sull'uso di tecnologie digitali e della rete Internet. Questo, però, non implica che l’individuo venga ridotto a semplice utilizzatore passivo di dispositivi elettronici. Al contrario, l’essere umano rimane al centro di queste attività, purché in possesso delle competenze necessarie per cercare e sfruttare con efficacia le informazioni disponibili online. L’agente segreto moderno deve quindi padroneggiare con facilità strumenti come

[1] A,Teti, *Cyber espionage e cyber counterintelligence : spionaggio e controspionaggio cibernetico Cyber Espionage e Cyber Counterintelligence*, Rubbettino Editore, 2018, p.5,6

smartphone, tablet, software e social network, che rappresentano oggi i principali mezzi di generazione e circolazione delle informazioni. Un'altra caratteristica distintiva dello spionaggio informatico è la sua economicità: con un piccolo gruppo di *hacker* esperti, alcune attrezzature informatiche e una connessione Internet stabile, è possibile orchestrare operazioni di cyberspionaggio di vasta portata. Le motivazioni dietro tali azioni variano e spaziano da obiettivi militari e ideologici a interessi economici, industriali, politici e sociali. Gli *hacker,* in questo contesto, assumono un ruolo fondamentale nelle operazioni di spionaggio elettronico, conferendo a queste attività un'efficacia senza precedenti. L' *Hacking* (chiamato anche *cyber hacking*) è l'uso di mezzi non convenzionali o illeciti per ottenere l'accesso non autorizzato a un dispositivo digitale, un sistema di elaborazione o una rete informatica. Gli *hacker* hanno sviluppato un mercato internazionale del crimine informatico che trae profitto dal lancio di attacchi informatici. Nel contesto della sicurezza informatica, i termini "hacking" e "attacco informatico" sono spesso utilizzati in modo intercambiabile, ma in realtà si riferiscono a concetti distinti, che rivestono ruoli e implicazioni differenti. L'hacking si riferisce all'insieme di tecniche e metodologie utilizzate per esplorare, manipolare o bypassare i sistemi informatici. Si tratta di un'attività che non è intrinsecamente malevola: l'hacker è colui che possiede una profonda conoscenza dei sistemi e delle loro vulnerabilità, e che è in grado di sfruttare tali conoscenze per accedere a risorse che altrimenti sarebbero inaccessibili. Tuttavia, l'hacking può assumere connotazioni diverse a seconda degli scopi e delle intenzioni dell'hacker stesso. L'attacco informatico, invece, è un'azione deliberata e mirata che ha lo scopo di compromettere l'integrità, la disponibilità o la riservatezza di un sistema informatico o dei dati che esso contiene. Gli attacchi informatici sono, per definizione, atti malevoli che mirano a danneggiare, distruggere, rubare o alterare dati e sistemi informatici. Esempi di attacchi informatici possono essere i *malware: software* dannosi progettato per infiltrarsi, danneggiare o disabilitare i sistemi. Esempi comuni sono virus, worm, trojan e ransomware o il *Phishing:* attacco che utilizza tecniche di ingegneria sociale per indurre gli utenti a fornire informazioni sensibili, come credenziali o dati bancari. La differenza fondamentale tra hacking e attacco informatico risiede quindi nell'intenzione e nell'approccio. L'hacking, pur implicando l'accesso non autorizzato a sistemi o risorse, non è necessariamente malevolo e può essere

utilizzato per migliorare la sicurezza informatica attraverso la scoperta e la correzione di vulnerabilità. Gli attacchi informatici, al contrario, sono sempre dannosi e mirano a compromettere la sicurezza o a trarre vantaggi illeciti, come il furto di dati, il danneggiamento di infrastrutture o l'estorsione, mentre l'hacking è una pratica che può avere sia applicazioni legittime che illecite, un attacco informatico è per definizione un'azione ostile e illegale. Nell'ambito della cybersicurezza e dello spionaggio informatico, comprendere questa distinzione è essenziale per formulare strategie di difesa efficaci e promuovere una maggiore consapevolezza tra utenti e organizzazioni. [2]

## 2 Normativa internazionale in materia di cyberspionaggio

Nel diritto internazionale una normativa ad hoc sullo spionaggio informatico non è universalmente accettata. Data la crescita esponenziale degli attacchi in informatici in tutto il mondo, degli studiosi di diritto internazionale hanno elaborato il Manuale di Tallin che fornisce delle linee guida circa l'applicabilità delle categorie del diritto internazionale alle *cyber-operation*[3]. Il manuale di Tallin ha lo scopo di creare il primo testo in materia di *cyber-warfare,* nonostante non ha assunto valore giuridico è stato riconosciuto come testo di riferimento poiché collega il diritto internazionale classico quello pattizio e quello consuetudinario, rappresenta l'opinio juris di giuristi inglesi pubblicato dal *Cambridge University press*.[4] Il lavoro è stato realizzato in un contesto ben definito e strategico: il gruppo di studio fa parte di un progetto del Cooperative Cyber Defence Centre of Excellence (CCDCOE), uno dei centri di eccellenza della NATO con sede a Tallin, Estonia. Già durante il summit NATO di Riga nel 2006, si era riconosciuta la pericolosità di possibili attacchi informatici, inseriti tra le minacce asimmetriche, e si era condivisa l'esigenza di elaborare iniziative a lungo termine per rafforzare (M.Kosinski, 2024) (L.Di.Pietro, 2013) (F.Sironi, 2019)la sicurezza e la protezione dei sistemi informatici. In questo scenario si è poi concretizzato il

[2] *M. Kosinski, Che cos'è l'hacking, 2024, www.ibm.com,*
[3] *Cyber operation. Operazioni che mirano unicamente a degradare in maniera attiva le capacità di un avversario i cui cyber-attacchi siano imminenti o in atto. Le cyberoperations sono strettamente legate al concetto di guerra cibernetica (cyberwarfare) e spionaggio informatico, ma si estendono anche a operazioni di influenza e sabotaggio digitale. In un contesto militare, sono spesso parte di strategie più ampie per il dominio dell'informazione e della sicurezza nazionale.*
[4] *L. Di Pietro, Il manuale di Tallin: diritto e cyber war, 2013, cesi-italia.org,*

CCDCOE, istituito a seguito dell'attacco cibernetico senza precedenti subìto dall'Estonia nell'aprile 2007, un evento definito da molti come un'operazione scientificamente progettata per colpire obiettivi specifici, individuati all'interno di strutture critiche. Il centro, inizialmente formato da Estonia, Lettonia, Lituania, Germania, Italia, Spagna e Slovacchia, si è successivamente ampliato includendo anche Polonia, Ungheria, Paesi Bassi e Stati Uniti. Pur mantenendo il ruolo di sponsoring nation esclusivamente per i Paesi NATO, il CCDCOE è aperto anche a collaborazioni con Stati non membri, università, istituti di ricerca ed imprese. L'obiettivo principale del centro è quello di potenziare le capacità di condivisione, cooperazione e scambio informativo nel settore della cyber-difesa, attraverso specifici programmi di istruzione, ricerca e sviluppo che si basano sull'esperienza pratica e sulla diffusione di conoscenze tra i partecipanti. Va inoltre precisato che, pur essendo uno strumento molto apprezzato nel settore, il "Tallin Manual" non rappresenta un documento ufficiale della NATO e, per questo motivo, non rispecchia necessariamente la posizione ufficiale dell'alleanza né di tutti i suoi membri. Tuttavia, gli esperti del settore lo valutano positivamente, considerandolo uno dei riferimenti giuridici più importanti in materia di cyber-war, particolarmente utile per chiarire vari aspetti applicativi. Questo quadro operativo e collaborativo, caratterizzato dall'impegno del CCDCOE e dalla diffusione di documenti come il Tallin Manual, evidenzia come la cooperazione internazionale e la condivisione delle conoscenze rappresentino elementi fondamentali per affrontare le sfide poste dalla crescente complessità della cyber-difesa e, più in generale, dello spionaggio informatico avendo come fine ultimo quello di costituire il primo corpus normativo relativo alla guerra cibernetica. La prima versione è stata pubblicata nel 2013 e successivamente aggiornata nel 2016, con un cambio di focus dalla "*cyber-warfare*" alle più ampie "*cyber-operations"*, riflettendo l'aumento di attacchi informatici che minacciano la sicurezza nazionale su base quasi quotidiana. Fin dall'introduzione, viene sottolineato che il Manuale rappresenta un'espressione delle opinioni di esperti, fornendo una fotografia del diritto internazionale vigente al momento della sua pubblicazione, senza porsi come guida normativa definitiva né come un passo avanti nello sviluppo del diritto. Il testo si autodefinisce come una determinazione oggettiva della lex lata (diritto vigente). In questa ottica, il Manuale rilegge il diritto internazionale stabilendo analogie tra il mondo fisico e quello cibernetico,

partendo dal presupposto che gli attacchi informatici condividono diverse caratteristiche con gli attacchi cinetici, soprattutto per quanto riguarda le conseguenze sulla vita umana, sull'integrità fisica e sulla distruzione di beni pubblici o privati. Inoltre, poiché le operazioni cibernetiche sono per loro natura transnazionali, la loro regolamentazione si inserisce a pieno titolo nel diritto internazionale. Gli esperti hanno identificato possibili comportamenti statali nel cyberspazio e li hanno interpretati secondo il diritto vigente, adottando una metodologia classica di diritto internazionale per proporre soluzioni. La versione 2.0 del Manuale, pubblicata nel 2016, è strutturata in quattro sezioni per un totale di 154 articoli (rules). Ciascuna regola è accompagnata da un commento giuridico che ne illustra l'applicazione pratica e offre esempi concreti. In caso di disaccordo tra gli esperti, i commenti alle regole spiegano il processo decisionale e le motivazioni alla base delle scelte adottate. La prima sezione del Manuale si concentra sui principi fondamentali del diritto internazionale applicabili al cyberspazio, definendo regole in materia di sovranità, giurisdizione e responsabilità statale. Le altre sezioni esplorano l'intersezione tra il cyberspazio e specifiche aree del diritto internazionale, come la tutela dei diritti umani, il diritto consolare, la regolamentazione aeronautica internazionale e il diritto del mare. Le ultime due sezioni trattano i temi tradizionali del diritto umanitario e dell'uso della forza, cercando di coniugare i principi del diritto internazionale con le sfide poste dalle nuove tecnologie in contesti di guerra e crisi internazionali. Un aspetto centrale è la legittimità dell'uso della forza come difesa contro attacchi cibernetici che, per intensità e modalità, possono rientrare nella definizione di attacco armato secondo il diritto internazionale. Al contrario, l'uso della forza come contromisura nei confronti di cyber-attacchi che non raggiungano la soglia di un attacco armato è una possibilità molto più limitata e rara, sebbene sia una situazione più frequente nella pratica. Uno dei temi più rilevanti affrontati nel Manuale riguarda il cyber-spionaggio, che viene analizzato in relazione alla sovranità statale e alla responsabilità internazionale. Lo spionaggio cibernetico, pur non essendo considerato un uso diretto della forza, può violare norme di diritto internazionale, in particolare quando compromette la sovranità di un altro Stato o viola trattati internazionali che regolano il comportamento degli Stati in tempo di pace e di guerra. Il cyber-spionaggio è strettamente legato a operazioni di *hacking* e infiltrazioni nei sistemi informatici per rubare informazioni sensibili di natura

politica, economica o militare. In un contesto globale sempre più dipendente dalla tecnologia, la sottrazione di dati tramite attacchi informatici rappresenta una minaccia continua alla sicurezza nazionale e internazionale. Il Manuale di Tallinn si impegna a fornire linee guida agli Stati su come rispondere a tali minacce. Anche se il cyber-spionaggio non raggiunge spesso il livello di un attacco armato, le sue implicazioni possono essere devastanti, mettendo in pericolo non solo la sicurezza di una nazione, ma anche la sua economia e il suo potere diplomatico. Il testo suggerisce quindi approcci per affrontare il cyber-spionaggio all'interno del quadro del diritto internazionale, con un occhio particolare alla cooperazione internazionale e allo sviluppo di normative che rafforzino la sicurezza informatica a livello globale. Nonostante l'importanza del Manuale, non mancano le critiche. Una delle più frequenti riguarda la visione occidentale adottata dagli esperti nella formulazione delle regole. Va precisato che, pur essendo stato elaborato all'interno di un centro di eccellenza NATO, i risultati non riflettono posizioni ufficiali dell'Alleanza e non vincolano i suoi membri. Un'altra critica significativa è l'approccio del Manuale nel trattare il cyberspazio come un "nuovo spazio fisico" da regolamentare come la terra, il mare o l'aria, con la possibilità per uno Stato di esercitarvi sovranità. In realtà, il cyberspazio sfugge in gran parte al controllo statale, poiché il flusso di dati attraversa confini fisici con facilità, rendendo difficile applicare le stesse regole del diritto internazionale che regolano lo spazio fisico. Il Manuale di Tallinn si distingue per la sua completezza nell'affrontare le problematiche giuridiche legate al cyberspionaggio e ad altre forme di attacchi cibernetici, proponendo un quadro di [5]riferimento utile per gli Stati che cercano di proteggersi da tali minacce. Offre una reinterpretazione delle Convenzioni di Ginevra nell'era delle tecnologie emergenti, come l'intelligenza artificiale e le armi autonome, e fornisce indicazioni su come gli Stati dovrebbero implementare regolamentazioni nazionali per rafforzare la propria sicurezza informatica. Nonostante alcune critiche, il Manuale rimane uno strumento fondamentale per comprendere e gestire i complessi problemi legati al cyberspazio e al cyberspionaggio, nel momento in cui viene suffragato da opportuna e sufficiente prassi può costituire fonte di diritto internazionale.

[5] *F.Sironi De G* (M.Manzari, 2020) (M.Cartisano, 2024)*regorio, Il Manuale di Tallin, 2019, www.cyberlaw.it,*

## 2.1 La Convenzione di Budapest sul Cybercrime

La Convenzione di Budapest viene conclusa nel 2001 sotto l'egida del Consiglio d'Europa con l'intento di raggruppare un catalogo di reati commessi attraverso internet. Questa Convenzione è il frutto di un lavoro trans-nazionale del *cybercrime,* mira alla cooperazione nazionale tra gli stati che ratificano la Convenzione. É il primo trattato internazionale che si occupa specificamente dei crimini informatici. È stata aperta alla firma il 23 novembre 2001 a Budapest ed è entrata in vigore il 1º luglio 2004. Questo trattato rappresenta un quadro giuridico internazionale di riferimento per contrastare il crimine informatico, e costituisce una pietra miliare nella regolamentazione delle attività criminali che coinvolgono le tecnologie informatiche. Detta Convenzione ha come obiettivo principale quello di armonizzare le leggi nazionali in materia di crimine informatico, facilitando la cooperazione internazionale tra gli Stati e migliorando le capacità investigative delle forze dell'ordine. In particolare, si concentra sun aspetto fondamentale quale la definizione dei crimini informatici che vanno dalla frode informatica al danneggiamento dei dati, includendo anche lo spionaggio informatico. Questi reati possono essere suddivisi in diverse categorie: Reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici, come l'accesso illecito, l'intercettazione illegale e il danneggiamento dei dati; reati legati all'uso improprio delle tecnologie informatiche, come la produzione e la distribuzione di virus, malware e altri strumenti dannosi reati legati al contenuto, come la distribuzione di materiale pedopornografico reati legati alle frodi informatiche. Un passaggio fondamentale della Convenzione è la cooperazione tra gli stati che aderiscono sia per l'assistenza giuridica reciproca nelle indagini, che per l'estradizione dei sospetti. Questo aspetto è particolarmente rilevante per il cyberspionaggio, in quanto molti attacchi informatici coinvolgono attori che operano da più giurisdizioni. La cooperazione internazionale consente di superare le barriere nazionali nella lotta ai crimini informatici permettendo un coordinamento più efficace tra le autorità. Si ha l'introduzione di strumenti giuridici per facilitare le indagini sui crimini informatici, come la possibilità di conservare e raccogliere rapidamente i dati informatici, compresi i dati relativi al traffico e alla localizzazione. Queste disposizioni sono essenziali per le indagini su crimini complessi come il cyberspionaggio, che spesso richiedono l'analisi di grandi quantità di dati e il monitoraggio in tempo reale delle comunicazioni. Nel

contesto del cyberspionaggio, la Convenzione di Budapest è un riferimento chiave per comprendere come la comunità internazionale stia affrontando il fenomeno dello spionaggio informatico. Sebbene non lo tratti direttamente, le disposizioni relative all'accesso illecito, all'intercettazione illegale e al danneggiamento di dati e sistemi informatici si applicano direttamente alle attività di spionaggio condotte attraverso mezzi informatici. Lo spionaggio informatico, infatti, rientra in molte delle categorie di crimini informatici descritte nella Convenzione. Gli Stati firmatari sono obbligati a criminalizzare queste condotte, il che ha un impatto diretto sulla lotta contro lo spionaggio informatico perpetrato sia da attori statali che da gruppi privati. Nonostante la sua importanza, la Convenzione di Budapest presenta anche dei limiti come la partecipazione limitata, molti stati non hanno aderito come Russia e Cina, nonostante siano importanti attori nel cyberspazio. Questo crea delle lacune nella cooperazione globale contro il crimine informatico e, di conseguenza, limita l'efficacia della Convenzione nel contrastare il cyberspionaggio a livello mondiale. Il rapido avanzamento delle tecnologie informatiche e delle minacce associate richiede aggiornamenti continui del quadro normativo, e la Convenzione, seppur pionieristica, può risultare datata in alcuni suoi aspetti rispetto alle tecniche più avanzate di spionaggio informatico. Tuttavia, per far fronte a queste minacce in evoluzione, è necessario un costantane aggiornamento delle normative, specialmente con l'integrazione di nuovi attori come l'intelligenza artificiale. [6]

[6] *M.Manzari, La Convezione di Budapest, L'Alba di una normativa di contrasto efficace al cybercrime, 2020, Bari*

## 2.2 Convenzione Onu contro i crimini informatici

In seguito alla Convenzione di Budapest del 2001, l'Organizzazione delle Nazioni Unite ha avviato un percorso per elaborare una propria Convenzione sulla criminalità informatica, con l'obiettivo di aggiornare e ampliare il quadro normativo globale per contrastare le minacce informatiche. [7] Il nuovo trattato, mira a colmare le lacune lasciate dalla Convenzione di Budapest, non ratificata da molti Paesi, tra cui Cina e Russia[8]. Questo trattato ONU necessita della ratifica di almeno 40 Stati per entrare in vigore. La Convenzione ONU mette al centro la lotta internazionale alla criminalità informatica, sottolineando come questa richieda una stretta collaborazione tra Stati. Si pone particolare attenzione su crimini come la pornografia infantile e il riciclaggio di denaro, e si introducono procedure per l'indagine e la gestione dei dati informatici in tempo reale. Inoltre, il trattato stabilisce l'obbligo per gli Stati membri di collaborare con uno scambio regolare di informazioni e, ove necessario, con il sequestro dei proventi di reato, garantendo assistenza legale reciproca nelle procedure di indagine ed estradizione. Uno degli obiettivi chiave del trattato è mantenere un costante aggiornamento rispetto all'evoluzione tecnologica, colmando il divario normativo di oltre vent'anni. Per questo motivo, già nel 2019 è stato istituito il *Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose* per affrontare la criminalità informatica in modo sistematico. I negoziati hanno avuto inizio nel 2017 e nel 2022 il comitato si è riunito per la prima volta per discutere e finalizzare il testo della Convenzione. Il trattato pone anche enfasi sull'uso legale e protettivo delle nuove tecnologie, come l'intelligenza artificiale (IA), sottolineando la necessità di bilanciare la sicurezza nazionale e la privacy individuale. Sebbene

[7] *M.Cartisano, Trattato globale Onu sulla Criminalità informatica, 2024,*

[8] *La posizione russa in materia di legislazione sulla criminalità informatica si basa prevalentemente su normative nazionali e su accordi bilaterali o multilaterali che non rientrano nel quadro della Convenzione di Budapest. La Russia ha sviluppato il proprio sistema giuridico per affrontare le sfide poste dal cybercrime, adottando leggi specifiche e misure di sicurezza, ma questo approccio è stato spesso criticato dalla comunità internazionale perché, secondo molti osservatori, tende a enfatizzare la sovranità nazionale a scapito di standard comuni condivisi a livello globale.*
*Inoltre, la Russia ha espresso riserve riguardo ad alcuni aspetti della Convenzione di Budapest, in particolare quelli relativi all'extraterritorialità e alla possibile limitazione della propria autonomia legislativa nel settore della sicurezza informatica. Per questi motivi, la Russia preferisce perseguire una strategia basata su normative interne e collaborazioni bilaterali, piuttosto che aderire a trattati multilaterali come quello di Budapest.*

l'IA possa rivelarsi uno strumento potente per individuare e tracciare attività sospette, la Convenzione invita i Paesi a introdurre linee guida rigorose per garantire che i dati sensibili siano raccolti e processati solo quando strettamente necessario. La trasparenza nei processi decisionali dell'IA è fondamentale: ogni decisione algoritmica dovrebbe essere documentata e soggetta a revisioni periodiche da parte di enti indipendenti, per evitare monitoraggi invasivi o ingiustificati. Per prevenire l'abuso di tecnologie avanzate a scopo di sorveglianza o controllo politico, il trattato ONU propone la definizione di standard internazionali condivisi. Questi standard faciliterebbero l'adozione di protocolli chiari, che prevengano l'uso dell'IA come strumento di repressione, garantendo invece un impiego uniforme e responsabile delle tecnologie di sicurezza. La Convenzione ONU rappresenta quindi un passo essenziale verso una regolamentazione dell'IA che protegga la sicurezza globale e rispetti i diritti umani, prevenendo abusi nei contesti di cyberspionaggio e altri crimini digitali.

## 2.3 Normativa a livello europeo: Direttiva Nis sul Cybercrime e GDPR

La Direttiva NIS (*Network and Information Security*), NIS rappresenta uno dei principali strumenti per migliorare la sicurezza delle reti e delle informazioni nell'UE, ponendo specifici obblighi di sicurezza per gli operatori di servizi essenziali (come trasporti, energia, banche) e i fornitori di servizi digitali. Adottata nel 2016 e successivamente aggiornata nella versione NIS2 nel 2022 estende la sua applicazione a più settori, introduce requisiti di sicurezza più stringenti e impone alle aziende di segnalare tempestivamente ogni incidente di sicurezza significativo. Il Framework NIS istituito nel 2016 ha segnato un passo decisivo verso l'armonizzazione degli statti membri nel settore della sicurezza delle reti e dei sistemi di informazione, rientra nel c.d. pacchetto digitale del 2016 in cui il legislatore europeo ha disciplinato la protezione dei dati personali. Gli obbiettivi che si è preposta sono quello di obbligare tutti gli Stati Membri ad adottare una normativa in materia di sicurezza informatica, agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati Membri, creare una rete di intervento per la sicurezza informatica detta CISRT in caso di incidente e i SOC, Centri Operativi di Sicurezza con la finalità di intervenire e prevenire gli attacchi informatici ed infine obbligare gli Stati Membri ad istituire autorità nazionali

competenti. Dalla direttiva possiamo estrapolare una definizione molto importante, quella di incidente informatico.[9] Tali incidenti dovranno essere comunicati all'autorità competente o al CISRT senza indebito ritardo. Nel gennaio 2023 è entrata in vigore la NIS2 sostituendo la direttiva 1148/2016 con focus sulla prevenzione e notifica degli incidenti. Le autorità nazionali degli Stati membri sono chiamate a cooperare tra loro e con le autorità di altri Paesi, contribuendo a creare un fronte unico contro i tentativi di cyberspionaggio che coinvolgono attori globali. Inoltre, il requisito di segnalazione degli incidenti aiuta a costruire un database di intelligence cibernetica, che gli Stati membri possono utilizzare per identificare pattern comuni e bloccare in modo preventivo attività di spionaggio informatico. La sicurezza informatica è considerata un elemento essenziale per permettere alle persone di fidarsi delle tecnologie digitali, di sfruttare appieno la connettività e di trarre vantaggio dai progressi tecnologici come l'automazione. Secondo il comunicato ufficiale, migliorare la cyber sicurezza è cruciale per proteggere non solo l'integrità delle infrastrutture digitali, ma anche i diritti e le libertà fondamentali dei cittadini. Questo include la salvaguardia della riservatezza, la tutela dei dati personali e la difesa della libertà di espressione e informazione. L'obiettivo primario della strategia europea è, quindi, quello di incrementare la capacità di resistenza collettiva dell'Unione Europea contro le minacce *cyber,* permettendo ai cittadini e imprese di accedere a un ecosistema digitale affidabile e sicuro. I punti chiave esposti nella direttiva sono energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio, la direttiva inoltre indirizza gli stati membri all' adozione di una strategia per neutralizzare i rischi proveniente dal cyberspazio. Un'altra importante introduzione è il regolamento che istituito nel 2021 ha dato vita ad un nuovo Centro di competenza per la *cyber security* e una rete di centri nazionali di coordinamento. Il Centro, con sede a Bucarest, contribuisce a rafforzare le capacità europee di *cyber security* e a promuovere l'eccellenza della ricerca e la competitività dell'industria dell'Unione nel settore. Con l'avvento di internet, dei social media, del cloud

[9] *Incidente informatico. Per incidente informatico si intende qualsiasi evento dannoso o pericoloso che compromettono la disponibilità, integrità o riservatezza dei dati conservati o trattati. Nella nozione rientra il fatto-reato indipendentemente dalla circostanza che sia commesso nell'interesse a vantaggio o danno degli operatori dei servizi essenziali. La rilevanza dell'impatto di un incidente tiene conti di determinati parametri quali: il numero di utenti interessati dalla perturbazione del servizio essenziale, la durata dell'incidente, la diffusione geografica dell'incidente*

computing e delle tecnologie, la quantità di dati raccolti e gestiti da aziende, enti pubblici e privati è aumentata in maniera incontrollata. Molti di questi dati erano trattati senza trasparenza, lasciando spazio a pratiche abusive e a una scarsa protezione contro il furto o l'accesso non autorizzato. Gli attacchi informatici e lo spionaggio digitale hanno raggiunto proporzioni allarmanti, spesso utilizzando dati personali per attività illecite come il furto d'identità, il monitoraggio non autorizzato, il sabotaggio economico o il ricatto. Introdotto dall'Unione Europea con il Regolamento UE 2016/679 il Regolamento Generale sulla Protezione dei Dati (GDPR), è nato dalla necessità di fornire una risposta efficace alle crescenti sfide poste dalla digitalizzazione e dalla globalizzazione. La trasformazione digitale ha ampliato in modo esponenziale la quantità di dati personali raccolti, archiviati e condivisi, rendendo tali informazioni una risorsa strategica ma anche una vulnerabilità. Lo scopo principale del GDPR è stato quello di rafforzare la tutela dei dati personali, garantendo al contempo la sicurezza informatica e promuovendo una maggiore consapevolezza sui diritti degli individui nel mondo digitale. Detto regolamento è attuabile dal 25 maggio 2018, uniforma tutte le normative degli stati membri in materia di trattamento dei dati personali effettuando un coordinamento tra il Garante Europeo che formerà nel tempo una base di prassi per il trattamento dei dati in ambito UE e i Garanti Nazionali che possano adottare provvedimenti prescrittivi inerenti al trattamento di specifiche tipologie di dati personali. I sette principi del trattamento dati sono:

- Liceità e correttezza
- Trasparenza
- Limitazione delle finalità dei trattamenti
- Minimizzazione
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza

Il Regolamento si applica al "trattamento interamente o parzialmente automatizzato dei dati personali ed al trattamento non automatizzato di dati personali contenuti in archivio. Il GDPR non stabilisce nello specifico a chi si applica, ma elenca invece espressamente a chi NON si applica e, cioè, tiene fuori dal proprio perimetro i trattamenti di dati personali:

- Relativi ad attività che non sottostanno al diritto dell'Unione;
- Effettuati da una persona fisica per attività personali o domestiche;
- Effettuati dalle autorità competenti ai fini di prevenzione, indagine, accertamento o perseguimento di reati (questi sono materia del D.Lgs. 51/2018 che, con regole molto simili, ha per destinatari le autorità competenti ma consente specifiche situazioni di trattamento senza consenso).

Dunque, il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; è quindi colui che acquisisce il dato o per conto del quale il dato viene acquisito, si dichiara nella «informativa» resa all'interessato. Il titolare porta con sé la responsabilità giuridica dell'intera filiera del trattamento, anche se delega i compiti a responsabili/autorizzati, salvo dimostrare di aver adottato tutte le misure necessarie e adeguate a consentire la sicurezza del trattamento. Analizzando i singoli articoli presenti nel GDPR vediamo come appunto l'art 33 tratti dei cc.dd *data breach*, la violazione dei dati personali. Detta violazione comporta: la perdita, la modifica, la divulgazione dei dati personali non autorizzati. La notifica fi questa eventuale violazione dovrà avvenire entro le successive 72 ore da quando il titolare ne è venuto a conoscenza, l'eventuale ritardo necessiterà una motivazione. Il Regolamento incoraggia l'uso di tecniche come la minimizzazione dei dati e l'anonimizzazione, principi che mirano a limitare la quantità di informazioni raccolte e a trasformarle in modo che non siano immediatamente riconducibili a individui specifici. Queste pratiche riducono il valore delle informazioni per i cybercriminali e i gruppi di spionaggio, rendendo più difficile per loro sfruttare i dati sottratti. L'articolo 32 del GDPR impone a tutte le organizzazioni che trattano dati personali di adottare misure tecniche e organizzative adeguate a garantire la sicurezza dei dati. Questo include l'uso di tecnologie avanzate come la crittografia, il controllo degli accessi e sistemi di monitoraggio per prevenire violazioni, strumenti indispensabili anche contro il cyberspionaggio. A rafforzare ulteriormente il sistema di protezione introdotto dal GDPR vi sono le sanzioni dissuasive, che possono raggiungere il 4% del fatturato globale o 20 milioni di euro. Queste pene rappresentano un incentivo significativo per le organizzazioni a investire nella sicurezza informatica, riducendo le

vulnerabilità che spesso vengono sfruttate nello spionaggio. Infine, il Regolamento prevede il ruolo centrale delle autorità di controllo indipendenti, responsabili di vigilare sul rispetto delle normative e di intervenire in caso di violazioni. Queste autorità, oltre a garantire la protezione dei dati personali, possono collaborare con altre istituzioni e agenzie per contrastare fenomeni di cyberspionaggio, che spesso coinvolgono attori statali e criminali organizzati. In questo contesto, il GDPR non è solo uno strumento per la tutela della *privacy,* ma si configura come una barriera normativa che protegge cittadini, aziende e governi dalle minacce del cyberspionaggio, promuovendo una cultura della sicurezza e della responsabilità digitale.

## 2.4 Ordinamento italiano, privacy vs protezione dei dati personali e normativa di riferimento

Nella Costituzione italiana non possiamo parlare specificamente di un diritto alla riservatezza (*privacy*), è pacifico però che esso ad oggi debba rientrare nella tutela costituzionale. Attualmente possiamo collegare il diritto alla riservatezza agli artt. 14,15,21 riferiti rispettivamente alla tutela del domicilio, alla segretezza della corrispondenza e alla libera manifestazione del pensiero. Il diritto alla riservatezza però trova le sue radici principalmente nell'art 2 della Costituzione italiana come diritto inviolabile dell'uomo. Un primo vero riconoscimento del diritto alla privacy si è avuto a partire dagli anni Settanta a seguito di un'importante pronuncia della Cassazione. Il legislatore è intervenuto prima con la Legge n. 675/1996 e poi con il d.lgs. n. 196/2003, il Codice della *privacy,* a seguito dell'adeguamento nazionale al regolamento UE. È necessario però effettuare una distinzione tra *privacy*, diritto alla riservatezza e protezione dei dati personali. I due che spesso, nel gergo comune, sono utilizzati come sinonimi in realtà presentano delle differenze. Il primo fa riferimento alla riservatezza delle informazioni personali della sfera fera privata dell'individuo principio usato come strumento per tutelare la sfera intima del singolo individuo volto ad impedire che le informazioni siano divulgate in assenza di specifica autorizzazione. La protezione dei dati personali invece, è uno sistema di trattamento degli stessi che identifica direttamente o indirettamente una persona e si collega al principio di disponibilità ed integrità dei dati personali. Nel contesto della tutela dei diritti individuali, si evidenzia una differenza significativa tra il concetto di privacy e quello di protezione dei dati personali, che affondano le loro radici in tradizioni

giuridiche diverse. La privacy è storicamente intesa come un mezzo per tutelare lo spazio privato da interferenze esterne, mentre la protezione dei dati personali pone l'accento sulla centralità della persona, considerata inseparabile dai propri dati, che rappresentano una componente fondamentale della sua identità. Dal punto di vista normativo, l'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea stabilisce la presenza di autorità di controllo indipendenti incaricate di garantire il rispetto delle norme sulla protezione dei dati. Questo si discosta dal modello statunitense, che privilegia l'autoregolamentazione, coerentemente con la filosofia liberista americana. Nel linguaggio comune, tuttavia, il termine "*privacy"* è spesso utilizzato in modo improprio per indicare anche la protezione dei dati personali, generando confusione. A tal proposito, persino il Garante per la protezione dei dati personali ha adottato il termine "Garante per la privacy" per favorire una migliore indicizzazione nei motori di ricerca. Questa sovrapposizione concettuale può contribuire alla percezione che il GDPR e le normative sulla protezione dei dati siano meri ostacoli burocratici per aziende e pubbliche amministrazioni. Tale visione può essere in parte attribuita all'approccio passato, legato a normative meno stringenti, come il Codice della privacy del 2003 e la Legge 675/1996, che prevedevano requisiti minimi rispetto alle prescrizioni più rigide introdotte dal Regolamento UE 2016/679 (GDPR) e dal DLgs. 101/2018. Analizzando il Codice della privacy istituito nel 2003, e seguentemente sostituito dal GDPR, si può evincere la confusione delle due definizioni. Il codice si occupava del trattamento dei dati personali, dei soggetti competenti, i diritti e le azioni di tutela che spettano al soggetto in questione. Detto codice aveva il compito di far si che la gestione dei dati personali avvenisse nel pieno rispetto dei diritti e libertà della persona, impone un elevato livello di tutela, fornendo anche il principio di necessità che riduce al minimo l'impiego dei dati personali, preferendo l'utilizzo di dati anonimi. Il Codice della *privacy* si concentrava in modo particolare sui limiti entro i quali tali dati possono essere utilizzati, con un'attenzione specifica ai dati sensibili. Tra i diritti riconosciuti al cittadino, in conformità al Codice in materia di protezione dei dati personali, emergono le seguenti facoltà:

- ottenere conferma dell'esistenza di dati personali che lo riguardano;
- essere informato sugli scopi per cui tali dati vengono trattati;
- richiedere l'aggiornamento o la rettifica dei propri dati;

- ottenere la cancellazione dei dati che sono trattati in violazione di legge o che non necessitano più di essere conservati.

Il Codice della privacy prevede inoltre, in determinati casi, l'obbligo di fornire l'informativa sulla privacy, come sancito dall'art. 13 del D.lgs. 196/2003. Tale disposizione stabilisce che l'interessato debba essere informato, oralmente o in forma scritta riguardo alle finalità del trattamento, ai soggetti a cui i dati personali possono essere comunicati, nonché alla natura obbligatoria o facoltativa del trattamento stesso. Il Codice era composto da 186 articoli e si divideva in 3 parti: Disposizioni genarli, Disposizioni relative a specifici settori e Tutela dell'interessato e sanzioni. A seguito del Decreto Monti del 2011, possono qualificarsi come dati personali solo quelli concernenti le persone fisiche e non anche quelli che riguardano le persone giuridiche o degli enti non riconosciuti, determinando una semplificazione della disciplina in tema di *privacy*.[10] In seguito alle nuove disposizioni normative introdotte dal Regolamento Europeo UE 2016/679 c.d. GDPR, detto regolamento sarà applicabile poi dal 25 maggio 2018. Nonostante la maggior parte degli articoli del Codice del 2003 furono abrogati, e la normativa di riferimento diventò il GDPR, il Codice rimane in vigore, lasciando intatte alcune parti del Codice quali ad esempio il Trattamento dei dati ai fini della sicurezza nazionale e della difesa o la protezione relativa al Garante della *privacy.*
Il diritto alla riservatezza e la protezione dei dati personali assumono un ruolo centrale nella lotta al cyberspionaggio, poiché questo fenomeno si basa proprio sull'acquisizione illecita di informazioni riservate, spesso appartenenti a individui, organizzazioni o enti governativi. L'articolo 2 della Costituzione italiana, che riconosce i diritti inviolabili dell'uomo, insieme alle disposizioni del GDPR, pone l'accento sulla necessità di salvaguardare non solo la privacy ma anche la sicurezza dei dati personali, specialmente in un contesto digitale. Lo spionaggio informatico viola sistematicamente questi principi, sottraendo dati sensibili che possono essere utilizzati per fini economici, politici o militari. Lo spionaggio informatico si realizza spesso attraverso l'accesso non autorizzato a sistemi informatici o reti, intercettazioni illecite e raccolta di dati sensibili. Queste attività mettono in pericolo non solo la riservatezza individuale ma anche la sicurezza

[10] (F.Oliva, 2017) (Maggio, 2024) (M.Tonellotto, 2020) (Ddl Cybersicurezza: così l'Italia rafforza le sue difese nel cyberspazio, 2024)*F.Oliva, Codice della Privacy: cosa prevede?, 2017, www.informazionediscale.it,*

nazionale e la competitività aziendale. Le normative sulla protezione dei dati, come il GDPR, includono obblighi specifici per proteggere i dati da violazioni e accessi non autorizzati, mirando a ridurre i rischi derivanti da attacchi informatici. La confusione tra privacy e protezione dei dati personali può avere un impatto negativo sulla percezione delle misure normative come strumenti di protezione contro il cyberspionaggio. Invece, è fondamentale sottolineare che normative come il GDPR, con i suoi principi di minimizzazione dei dati e trasparenza, costituiscono barriere contro l'acquisizione indebita di dati personali. Il Codice della privacy, mantenendo intatti articoli legati al trattamento dei dati per la sicurezza nazionale e la difesa, evidenzia come la protezione dei dati non riguardi solo gli individui, ma anche la tutela della sovranità digitale di un paese. Nel contesto dello spionaggio informatico, i dati rubati spesso riguardano informazioni strategiche che possono compromettere infrastrutture critiche o interessi geopolitici, l'intersezione tra il diritto alla riservatezza e il cyberspionaggio dimostra come la protezione dei dati personali non sia solo un diritto individuale, ma anche un elemento chiave per garantire la sicurezza collettiva e la sovranità degli stati nel panorama digitale globale. Inseguito analizzeremo l’istituzione a livello nazionale dell’Agenzia per la Cybersicurezza Nazionale e il Perimetro di Sicurezza Nazionale.

## 2.5 Il Perimetro di sicurezza nazionale e Il CAD e ACN Agenzia per la Cybersicurezza Nazionale

Con la legge 133 del 2019 al fine di assicurare un elevato sistema di sicurezza delle reti informatiche e dei servizi delle amministrazioni pubbliche e private da cui dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di un servizio essenziale per il mantenimento di attività economiche fondamentali per gli interessi dello stato e dal qual cui malfunzionamento o interruzione potrebbe arrecare un pregiudizio per la sicurezza nazionale, si istituisce il Perimetro di Sicurezza Nazionale Cibernetica. Gli operatori scelti dal Presidente del Consiglio dei ministri per operare nel Perimetro devono come requisiti:

- Esercitare una funzione essenziale dello Stato o assicurare un servizio essenziale per il mantenimento delle attività fondamentali dello Stato
- Essere dipendenti da reti o sistemi informativi per l'esercizio delle loro funzioni
- Causare in caso di malfunzionamento un pregiudizio grave alla sicurezza dello Stato

Un ruolo importante lo svolge il Centro di Valutazione e certificazione Nazionale, il quale presta garanzie alle strutture sottoposte a maggiore criticità nel funzionamento di sistemi e servizi informatici e contribuisce all'elaborazione di misure di sicurezza del Perimetro di Sicurezza Nazionale Cibernetica. Detto Perimetro si intrinseca perfettamente con il Framework NIS, gli operatori possono incorrere in delle sanzioni nel momento in cui non si conformano al d.l 105/2019 volti alla prevenzione degli incidenti e degli attacchi informatici. Seguentemente all'istituzione del PSNC in Italia si arriva ad una grande innovazione istituendo per la prima volta con il d.l 82/2021 l' Agenzia per la Cybersicurezza Nazionale, con sede a Roma. L'obbiettivo di questa agenzia è quello di unire tutte le competenze in materia di cybersicurezza che precedentemente erano assegnate a tutti i Ministeri sotto un'unica direzione facente capo al Consiglio dei ministri. L'ACN si occupa di esercitare tutte le materie di cybersecurity tutelando gli interessi nazionali e prevenendo le minacce cibernetiche, sviluppando anche capacità di monitoraggio di incidenti e attacchi informatici attraverso il *Computer Security Incident Response Team.* Inoltre, ha anche la funzione di supportare l'innovazione mirando alla crescita nel campo cyber e assumere il ruolo di

interlocutore unico per soggetti pubblici e privati nell'ambito della sicurezza nazionale cibernetica. Successivamente analizzeremo il legame che unisce la sicurezza nazionale e il cyberspazio.

## 3 Evoluzione del *Cyber Espionage* dal secondo dopoguerra ai giorni odierni

Dopo la fine della Seconda Guerra Mondiale le priorità dell'intelligence sono rimaste costanti ma hanno subito delle variazioni, adattandosi al cambiamento della società. La tecnologia ha permesso l'aumento degli attacchi e delle guerre informatiche sempre più numerose. Da ciò possiamo evincere il collegamento tra il *cyber espionage e la cyber war*. Nel contesto mondiale odierno la sicurezza nazionale è uno dei centri di interesse più importanti sui quali l'attività di *intelligence* adopera, le attività di *intelligence* non si limitano più soltanto alla difesa dello Stato, ma si estendono alla protezione della cittadinanza da minacce come terrorismo, crisi economiche e soprattutto *cyber war*, avendo una crescita esponenziale dei *cyber attack*[11], di ciò ne parleremo successivamente. Gli hacker agiscono come veri e propri soldati digitali e gli attacchi informatici vengono utilizzati come strumenti per compromettere la sicurezza nazionale del Paese avversario e ottenere vantaggi strategici. L'obbiettivo degli hacker è quello di sottrarre quante più informazioni possibili, che sono riservate o coperte da segreto di stato. Questi *cyber attack* sono molto complessi, infatti, è molto difficile difendersi da queste minacce. Le cyberspie hanno a loro disposizione ingenti quantità di denaro che gli vengono fornite dai governi ed è per questo che accedono a software molto sofisticati che gli permettono di sferrare gli attacchi. Analizzando l'evoluzione di questo fenomeno sin dagli arbori possiamo vedere come verso la fine degli anni '60 ha preso avvio l'epoca dei computer, inizialmente concepiti come strumenti elettromeccanici per risolvere complessi problemi di calcolo, specialmente nel campo della ricerca accademica e della difesa. Con il tempo, questi sistemi si sono evoluti in tecnologie digitali avanzate, trovando applicazione in ambiti come l'industria, il commercio, la finanza e la comunicazione globale, grazie anche alla crescente diffusione di Internet. Non appena si è capito che i computer potevano veicolare informazioni riservate e di

[11] *Cyber attack: è un tentativo di ottenere l'accesso non autorizzato ai sistemi informatici al fine di appropriarsi, modificare o distruggere dati.*

valore strategico, sono diventati subito un bersaglio ideale per operazioni di spionaggio. Il cyber-spionaggio, o spionaggio informatico che consiste nell'acquisire informazioni sensibili, personali o classificate attraverso il cyberspazio, senza il consenso o la consapevolezza del legittimo proprietario, permette alle intelligence di impossessarsi dei dati provenienti da individui, aziende, governi o istituzioni, che rappresentano un'enorme risorsa, poiché offrono vantaggi in ambito militare, economico, industriale, politico e sociale. Le tecniche di cyber-spionaggio si adattano agli obiettivi specifici, ma spesso includono l'uso di malware, trojan e spyware, oltre a metodologie di cracking. Un aspetto fondamentale di questa pratica è il reclutamento di persone con accesso diretto ai sistemi di interesse, fornendo loro gli strumenti necessari per sottrarre dati. Un altro approccio comune è lo studio delle vulnerabilità dei sistemi, attraverso test mirati e strumenti di analisi per capire come penetrarli. Già nel 1967, Willis Howard Ware, ingegnere e pioniere della tecnologia informatica, aveva sottolineato l'importanza di anticipare questi rischi. In un suo intervento, affermava: "Lo spionaggio cerca di ottenere informazioni militari o di difesa utilizzando anche notizie pubbliche. Ora che i sistemi di elaborazione elettronica sono ampiamente usati in ambito militare e difensivo, bisogna aspettarsi tentativi deliberati di infiltrarsi al loro interno." Questa intuizione mostra quanto, già agli albori dell'era digitale, fosse chiaro il potenziale dello spionaggio informatico e l'urgenza di sviluppare contromisure adeguate. L'osservazione di Ware anticipava una realtà che oggi è diventata una delle principali preoccupazioni per governi, aziende e organizzazioni internazionali. Con il progresso tecnologico e l'interconnessione globale, lo spionaggio informatico si è trasformato in una minaccia concreta e sempre più sofisticata, capace di colpire infrastrutture critiche, sistemi industriali e reti governative. Gli attacchi non si limitano più a sottrarre informazioni, ma mirano anche a sabotare processi fondamentali, alterare dati sensibili o compromettere la sicurezza di intere nazioni. Il contesto odierno è caratterizzato da una competizione globale per il controllo delle informazioni e delle tecnologie avanzate. Questo ha reso il cyberspazio un campo di battaglia strategico, dove gli attori principali non sono solo Stati, ma anche organizzazioni criminali, gruppi terroristici e aziende concorrenti. Ogni entità cerca di ottenere un vantaggio competitivo sfruttando le vulnerabilità dei sistemi digitali, sia attraverso attacchi mirati sia mediante il reclutamento di insider,

spesso motivati da ragioni economiche o ideologiche. Tra le tecniche più diffuse rientrano l'uso di malware progettati per infiltrarsi nei sistemi, rubare dati o danneggiare hardware e software; gli attacchi phishing, che sfruttano l'ingegneria sociale per ingannare le vittime; e l'uso di trojan, in grado di accedere a sistemi protetti mascherandosi da programmi legittimi. A ciò si aggiunge l'uso sempre più sofisticato dell'intelligenza artificiale, capace di automatizzare e rendere più efficaci le operazioni di spionaggio. Un esempio emblematico della portata del cyber-spionaggio è il caso del *malware* Stuxnet, scoperto nel 2010, che rappresenta la prima cyber-arma nota in grado di causare danni fisici a infrastrutture critiche. Questo software è stato utilizzato per sabotare centrifughe nucleari in Iran, dimostrando come un attacco informatico possa avere conseguenze devastanti anche nel mondo reale. Eventi come questo hanno spinto molti Paesi a riconoscere il cyberspazio come un nuovo dominio della conflittualità, al pari di terra, mare, aria e spazio. L'urgenza di proteggere le informazioni digitali e le infrastrutture critiche ha portato allo sviluppo di strategie nazionali e internazionali per la cyber-sicurezza, con l'obiettivo di prevenire, rilevare e rispondere a questi attacchi. Tuttavia, nonostante i progressi compiuti, le sfide rimangono enormi. La rapidità con cui evolvono le minacce informatiche richiede un adattamento continuo, oltre alla collaborazione tra Stati, aziende private e istituzioni per condividere informazioni e risorse. Alla luce di questi sviluppi, il cyber-spionaggio non è più solo una questione tecnica, ma un tema centrale nelle relazioni internazionali e nella geopolitica contemporanea. La capacità di difendere le proprie reti digitali e di rispondere a eventuali attacchi rappresenta una componente fondamentale per garantire la sicurezza nazionale, la stabilità economica e la competitività globale. Nel 1970, l'introduzione del *time-sharing* [12]ha permesso a più utenti di accedere simultaneamente allo stesso computer utilizzando modem collegati a linee telefoniche. Questa innovazione ha spinto a intensificare gli sforzi per integrare i modem nelle intercettazioni telefoniche e sottrarre le password necessarie per accedere ai sistemi di trasmissione dati. Con gli anni '80 e la nascita di Internet, i computer hanno iniziato a connettersi in rete, aprendo nuove possibilità per le agenzie di

[12] *Time-sharing Genericamente: la possibilità offerta a più utenti di attingere in tempi immediatamente successivi a risorse disponibili in scarsa misura; l'espressione (spesso resa in italiano con divisione di tempo,) è usata soprattutto nella tecnica degli elaboratori elettronici, per indicare il modo di funzionamento 'a multiprogrammazione' che consente a più utenti di utilizzare contemporaneamente un sistema di calcolo con programmi diversi*

intelligence di tutto il mondo. La rete offriva uno spazio ideale per condurre operazioni di spionaggio con maggiore sicurezza e nuove prospettive per le attività clandestine. Un esempio significativo di spionaggio informatico risale al 1986, quando un gruppo di hacker tedeschi, affiliati alla Stasi e supportati dal KGB, riuscì a infiltrarsi in centinaia di computer della rete militare statunitense MILNET. Questo episodio rappresenta una delle prime manifestazioni del potenziale del cyberspazio come terreno di competizione strategica. L'arrivo del *personal computer* IBM (uno dei primissimi computer) nel 1980 e la diffusione dell'architettura IBM compatibile hanno rivoluzionato il mercato tecnologico, consentendo a più produttori di entrare nel settore. Questo sviluppo ha favorito la creazione di sistemi operativi e applicazioni specifiche per la gestione d'ufficio e il business, ampliando ulteriormente l'uso dei computer sia in ambito lavorativo che domestico. Tra il 1980 e il 1990, l'interesse delle agenzie di intelligence per il mondo dei computer e delle reti è cresciuto rapidamente. I *Personal Computer*, ormai presenti sia in casa che in ufficio, contenevano dati personali e sensibili che potevano essere di grande utilità per le operazioni di spionaggio. Sebbene le tecniche di violazione informatica dell'epoca fossero rudimentali rispetto agli standard odierni, alcune innovazioni si sono rivelate particolarmente significative. Una di queste è il sistema *Tempest*, sviluppato dalla *National Security Agency (NSA)*. Questo programma, che prende il nome da un termine tecnico piuttosto che da un acronimo, si concentrava sull'analisi delle emissioni compromettenti prodotte dai dispositivi elettronici. Il sistema Tempest si basava sull'identificazione e la protezione dalle emissioni non intenzionali – come energia elettrica, suoni o onde elettromagnetiche – generate da dispositivi come monitor, computer e cavi di rete. Queste emissioni potevano essere intercettate e utilizzate per ricostruire i dati processati o trasmessi. La capacità di intercettare tali informazioni dipendeva da vari fattori, tra cui il rumore ambientale e il livello di sicurezza dei dispositivi. Questo tipo di ricerca rappresentava un tentativo pionieristico di affrontare le vulnerabilità delle tecnologie elettroniche, un tema che sarebbe diventato sempre più centrale con l'avanzare della rivoluzione digitale. Parallelamente, alla fine degli anni '80, sono comparse le prime botnet: reti di computer infettati da malware e controllate da remoto da un botmaster. Attraverso virus e trojan, i dispositivi venivano sfruttati per attacchi o per accedere a informazioni sensibili, dimostrando come i computer potessero agire come veri

e propri agenti segreti digitali. Questa evoluzione ha portato a un parallelismo tra le metodologie tradizionali di intelligence HUMINT e quelle del cyberspazio, dove le tecniche di reclutamento, infiltrazione e manipolazione sono adattate al contesto virtuale. Nel cyberspazio, l'intelligence gathering, ovvero la raccolta di informazioni si basa principalmente sull'utilizzo di malware installati su server compromessi, progettati per sfruttare le vulnerabilità dei sistemi informatici. Il *tradecraft*, termine che indica l'insieme di tecniche operative usate nello spionaggio, distingue le attività professionali di *cyber intelligence* dagli attacchi informatici comuni. Come dimostrato dalla comparazione tra HUMINT[13] e cyber intelligence, le strategie utilizzate nel reclutamento e nella manipolazione di fonti fisiche e digitali condividono molte somiglianze. Un caso rilevante di sorveglianza digitale è quello del software *Galileo* sviluppato dalla Hacking Team, un'azienda italiana il cui strumento di spionaggio è stato utilizzato da numerosi governi per monitorare dispositivi informatici e mobili, per permette di accedere a ogni tipo di dato sul dispositivo infettato, dalla geolocalizzazione ai messaggi e alle applicazioni utilizzate. La diffusione di botnet [14]e malware ha reso il cyberspazio un luogo popolato da agenti dormienti, sempre alla ricerca di informazioni riservate. Con l'avvento degli smartphone e la crescente connettività delle reti wireless, il flusso di comunicazioni digitali ha raggiunto livelli straordinari. Questo fenomeno si amplificherà ulteriormente con l'Internet delle Cose (IoT),[15] che collegherà dispositivi come elettrodomestici, automobili e gadget indossabili, creando nuove opportunità per lo spionaggio. Guardando all'evoluzione della tecnologia, possiamo tracciare un parallelo con il ciclo di vita delle stelle. I mainframe, che dominavano negli anni '80, erano enormi e potenti, ma con il tempo hanno ceduto il passo ai personal computer, più piccoli e veloci. Questi, a loro volta, hanno generato la rete Internet, dando vita a una nuova era tecnologica culminata con la nascita degli smartphone. Questa evoluzione continua oggi con l'IoT, che connetterà ogni aspetto della vita quotidiana, ampliando il panorama dello spionaggio e sollevando preoccupazioni sulla

---

*[13] HUMINT: è l'attività di intelligence consistente nella raccolta di informazioni per mezzo di contatti interpersonali e come tale si contrappone ad altri canali informativi più "tecnologici". La NATO definisce la HUMINT come una categoria di intelligence derivata da informazioni raccolte e fornite da fonti umane.*

*[14] Botnet: si intende una rete di computer infetta e controllata da un hacker da remoto da un botmaster cioè un hacker che l'ha istituita*

*[15] IOT: internet of things: è un neologismo utilizzato nel mondo dell'informatica per far riferimento all'estensione di internet al mondo domestico e luoghi concreti che acquistano identità digitale*

possibilità di un controllo sociale totalizzante, evocando scenari simili a quelli descritti da George Orwell in *1984*.[16]

## 3.1 Definizione di Sicurezza Nazionale nel Cyberspazio

Come detto precedentemente la sicurezza nazionale è uno dei centri di interesse più importanti sui quali l'attività di *intelligence* adopera. La sicurezza nazionale è stata tradizionalmente intesa in chiave militare, concentrandosi sulla capacità di un paese di proteggere i propri confini da attacchi armati. Tuttavia, le sfide del presente richiedono una revisione di questa visione limitata. Oggi, la sopravvivenza e la stabilità delle società, indipendentemente dal loro livello di sviluppo o industrializzazione, sono minacciate da fattori che vanno oltre le tradizionali considerazioni militari. Elementi come l'ambiente e l'instabilità interna rappresentano rischi concreti per la sicurezza di una nazione. In particolare, la prospettiva tradizionale fatica a incorporare adeguatamente le minacce provenienti dal cyberspazio. La sicurezza nel cyberspazio si riferisce alla capacità di uno Stato di proteggersi da attacchi cibernetici, spionaggio, sabotaggi, crimini informatici, frodi e altre minacce digitali. La cybersecurity, come la sicurezza ambientale, richiede un approccio che superi i tradizionali confini sociali e istituzionali. La crescente interconnessione globale e l'importanza strategica delle infrastrutture critiche rendono [17]evidente la necessità di adottare politiche di sicurezza cibernetica che superino i confini delle singole giurisdizioni nazionali. In quest'ottica, la sicurezza nazionale nel cyberspazio non può più essere concepita come una responsabilità esclusivamente statale, ma richiede un approccio condiviso, basato su una stretta cooperazione internazionale. Per garantire un'efficace prevenzione delle minacce, è indispensabile mettere in comune competenze e risorse, promuovendo attività di intelligence e investigazione basate sullo scambio costante di informazioni. Settori chiave come l'energia, i trasporti e le telecomunicazioni rappresentano punti nevralgici della sicurezza nazionale, poiché un attacco informatico rivolto a tali infrastrutture avrebbe inevitabili ripercussioni non solo sull'economia nazionale, ma anche sul sistema paese nel suo complesso. Gli eventi più recenti confermano quanto le

[16] *J.DiMaggio, L'arte della guerra informatica, 2024*
[17] *M.Tonellotto, Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità, 2020, Bologna,*

minacce alle infrastrutture critiche siano una realtà concreta e urgente. Senza un forte coordinamento internazionale, il rischio non si limita al danneggiamento interno, ma si estende anche alla stabilità geopolitica globale. La sicurezza cibernetica, dunque, diventa una componente imprescindibile della sicurezza nazionale, richiedendo soluzioni che integrino visione strategica, capacità tecniche e collaborazione tra Stati e organizzazioni sovranazionali. Nel gennaio 2024 è stato presentato un disegno di legge approvato poi dal Consiglio dei ministri, volendo rafforzare le misure nazionali contro i cybercrime e migliorando le strutture che sono comprese nel Perimetro di Sicurezza Nazionale Cibernetica. Il ddl Cybersicurezza mira a proteggere il sistema digitale e consolidare le difese. Il Disegno di Legge sulla Cybersicurezza introduce un insieme di misure strategiche volte a rafforzare la capacità di prevenzione e risposta dell'Agenzia per la Cybersicurezza Nazionale (ACN). Tra le novità principali, spicca il miglioramento del coordinamento con le autorità giudiziarie e l'introduzione di norme più rigide per contrastare i reati informatici. In caso di attacchi informatici che coinvolgano infrastrutture critiche per la difesa, la sicurezza nazionale, la sanità o altri servizi essenziali, il Disegno di Legge stabilisce un coordinamento stretto tra le autorità giudiziarie e il Sistema di Informazione per la Sicurezza della Repubblica. Questa collaborazione è fondamentale per gestire l'impatto degli incidenti, indagare le cause e pianificare azioni di mitigazione. Il Disegno di Legge pone un forte accento sull'uso dell'intelligenza artificiale (IA) per rafforzare la sicurezza cibernetica. L'ACN assume un ruolo di guida, promuovendo iniziative pubbliche e private per integrare l'IA nelle strategie di protezione, assicurandosi che il suo utilizzo sia etico e sicuro, con il supporto dell'AGID e del Dipartimento per la Trasformazione Digitale, lavora per garantire che l'IA sia progettata e utilizzata in modo sicuro, in linea con le migliori pratiche internazionali. In sinergia con le raccomandazioni del *National Cyber Security Centre* britannico, l'ACN ha adottato linee guida globali per lo sviluppo sicuro dell'IA, firmate da 23 agenzie di 18 Paesi. Queste indicazioni mirano a garantire che i fornitori di sistemi IA, sia nuovi che basati su piattaforme esistenti, adottino pratiche di sicurezza avanzate, creando un ambiente digitale più protetto per cittadini e istituzioni. L'approvazione del Disegno di Legge sulla Cybersicurezza rappresenta un passo significativo per migliorare la protezione del Paese contro le minacce digitali. Le nuove misure rafforzano le capacità di prevenzione,

rilevamento e reazione agli attacchi informatici, integrando normative più rigide e una maggiore cooperazione tra istituzioni. Questo quadro normativo contribuirà a migliorare la resilienza delle infrastrutture critiche, tutelando al contempo i dati sensibili dei cittadini e garantendo un cyberspazio più sicuro. [18]Nel capitolo seguente analizzeremo casistiche emblematiche in materia di cyber spionaggio da Wikileaks al Datagate, che hanno evidenziato come la raccolta e la divulgazione illecita di informazioni sensibili possano avere ripercussioni globali. Inoltre, si affronterà il tema dello spionaggio informatico nel contesto del conflitto russo-ucraino, un esempio recente e drammatico di come il cyberspionaggio sia diventato una componente chiave nei conflitti geopolitici moderni.

[18] Agenda Digitale, *Ddl Cybersicurezza: così l'Italia rafforza le sue difese nel cyberspazio, 2024*

# CAPITOLO II

# Spionaggio informatico nella pratica: Analisi di tre casi emblematici

## 1 Wikileaks e le sfide di diritto internazionale

WikiLeaks noto come un archivio digitale progettato per raccogliere e pubblicare documenti riservati, di natura governativa, militare, bancaria o industriale, garantendo l'anonimato di chi contribuisce al flusso informativo. Questo obiettivo è stato raggiunto attraverso l'adozione di avanzati sistemi di crittografia, volti a proteggere non solo gli informatori ma anche lo staff della piattaforma. Una delle peculiarità di WikiLeaks era l'assenza di una sede fisica ufficiale, il che la rendeva una sorta di "Wikipedia non tracciabile", dedicata alla pubblicazione e all'analisi su larga scala di documenti confidenziali. La piattaforma, il cui principale fondatore e volto pubblico è stato Julian Assange, ha avuto un impatto significativo sul panorama globale, mettendo in discussione il rapporto tra la libertà di informazione e la tutela della sicurezza nazionale. L'intento dichiarato di WikiLeaks era quello di promuovere la trasparenza e responsabilizzare governi e istituzioni, sebbene questo abbia portato a tensioni rilevanti nel contesto giuridico internazionale, specialmente in relazione alla protezione di informazioni classificate. Nel 2007, WikiLeaks raggiunse una nuova fase di sviluppo grazie al contributo di un attivista esperto del software Tor, che consentì alla piattaforma di intercettare e registrare il traffico dati di alcuni hacker cinesi intenti a raccogliere informazioni sui governi occidentali. Questo evento segnò una svolta cruciale, poiché fornì nuovo materiale riservato da pubblicare. Nello stesso periodo, lo staff della piattaforma annunciò l'intenzione di rilasciare oltre 1.200.000 documenti riservati, ponendo WikiLeaks al centro del dibattito globale sulla divulgazione di informazioni sensibili. [19]La pubblicazione di documenti di grande rilievo ebbe inizio nella seconda metà del 2007. Tra questi, spiccavano rivelazioni sulla gestione del campo di detenzione di Guantánamo e sull'equipaggiamento militare statunitense impiegato durante il conflitto in Afghanistan. Tali divulgazioni suscitarono un'immediata reazione da parte di governi e istituzioni. Nel 2008, il

[19] (Benkler.Y, 2011), (S, 2010) (Coleman.G, 2011) *Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate. Harvard Law Review, 2011, 46, pp. 311-394.*

sito fu temporaneamente chiuso su ordine di un tribunale californiano, in seguito alle pressioni esercitate dalla banca svizzera Julius Bär, coinvolta nella diffusione di documenti che la accusavano di agevolare pratiche di evasione fiscale. Tuttavia, pochi mesi dopo, il tribunale revocò tale decisione, consentendo a WikiLeaks di riprendere le proprie attività.[20] Un momento chiave nella storia della piattaforma fu la collaborazione, nel luglio 2010, con tre importanti testate giornalistiche internazionali: *The New York Times, The Guardian e Der Spiegel*. Attraverso queste partnership, WikiLeaks rese pubblici documenti riservati relativi alla guerra in Afghanistan. Tra le rivelazioni più significative figuravano rapporti sull'uccisione di civili e l'occultamento di cadaveri, l'operatività di un'unità segreta americana incaricata di eliminare fisicamente membri talebani senza processo, e la collaborazione occulta tra i servizi segreti pakistani e i leader talebani, nonostante il Pakistan fosse un alleato ufficiale degli Stati Uniti. L'impatto di queste divulgazioni fu di portata globale, sollevando interrogativi cruciali sul bilanciamento tra trasparenza e sicurezza. La vicenda si intreccia con il diritto internazionale sotto diversi aspetti: dalla violazione delle norme sulla segretezza diplomatica alla protezione dei whistleblower,[21] fino al ruolo delle istituzioni statali nella regolamentazione delle attività digitali transnazionali. Successivamente, Wikileaks affrontò un periodo di transizione. Nel 2010, l'uscita di scena di Daniel Domscheit-Berg, uno dei collaboratori principali, e l'arresto di Julian Assange nel Regno Unito segnarono una fase di inattività per la piattaforma. Nonostante ciò, WikiLeaks rimane un caso emblematico che continua a influenzare il dibattito giuridico e politico a livello internazionale, evidenziando le sfide che il cyberspionaggio e la divulgazione di informazioni sensibili pongono al sistema normativo globale.

[20] *Aftergood, S. The Impact of WikiLeaks on International Security,* Journal of Cyber Policy, 2010, 5*(2), pp. 145-167.*
[21] *Coleman, G, WikiLeaks: Whistleblowing in the Digital Age,* Journal of Information Technology & Politics, 2011, 8*(1), pp. 89-105* (M, 2017)

## 1.2 La sfida giuridica della pubblicazione dei documenti classificati da soggetti non statali

La pubblicazione di documenti classificati da parte di soggetti non statali rappresenta una delle sfide più complesse e controverse nel panorama contemporaneo della sicurezza informatica e del diritto internazionale. [22][23] Questo fenomeno consiste nella diffusione non autorizzata di informazioni riservate, spesso coperte da vincoli di segretezza di Stato, aziendale o personale, da parte di individui, gruppi o piattaforme che operano al di fuori delle strutture governative. L'obiettivo dichiarato di queste operazioni è spesso quello di promuovere la trasparenza e garantire la responsabilità istituzionale, ma le implicazioni legali, politiche e sociali che ne derivano sono estremamente complesse e polarizzanti. La pratica della pubblicazione di documenti riservati è resa possibile dall'evoluzione tecnologica, che ha rivoluzionato il modo in cui le informazioni vengono acquisite, trasmesse e diffuse. Tecnologie come le reti anonime, ad esempio Tor, e l'uso avanzato della crittografia consentono ai soggetti non statali di operare senza essere facilmente tracciati, garantendo al contempo la protezione delle loro fonti. Piattaforme globali come WikiLeaks, nate con l'intento di offrire uno spazio sicuro per la divulgazione di informazioni sensibili, hanno reso possibile la condivisione su scala mondiale di documenti in pochi istanti, bypassando i tradizionali canali di comunicazione e amplificando il loro impatto. In alcuni casi, le informazioni pubblicate provengono da attacchi informatici e violazioni di sistemi di sicurezza, come dimostrano esempi noti come il DNC Hack del 2016. Il fenomeno è intrinsecamente legato a questioni di trasparenza e a*ccountability*[24]. Gli attori coinvolti, come nel caso di *WikiLeaks,* giustificano le loro azioni sostenendo che la pubblicazione di documenti classificati sia necessaria per denunciare comportamenti illeciti, abusi di potere o pratiche non etiche da parte di governi, aziende o istituzioni. Julian Assange, fondatore di *WikiLeaks,* ha ripetutamente affermato che la trasparenza radicale è un requisito indispensabile per il corretto funzionamento della democrazia. Allo stesso modo, Edward Snowden ha motivato la sua decisione di rivelare i

[22] *Fenwick, M. et al. Shifting Meaning of Legal Certainty in Comparative and Transnational Law. Springer,2017,*
[23] *Lyon, D. Surveillance after Snowden. Polity Press,2015*
[24] Accountability: responsabilizzazione di titolari e responsabili, gli viene dato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento (GDPR).

programmi di sorveglianza di massa della National Security Agency (NSA) come un atto volto a difendere i diritti fondamentali delle persone, in particolare il diritto alla privacy. Tuttavia, questo tipo di trasparenza pone un dilemma etico e giuridico: se da un lato favorisce il controllo pubblico sull'operato delle istituzioni, dall'altro può mettere a rischio la sicurezza nazionale, le relazioni diplomatiche e, in alcuni casi, anche vite umane. La pubblicazione di documenti classificati da parte di soggetti non statali ha avuto numerosi esempi emblematici. Oltre al già citato caso WikiLeaks, il fenomeno ha visto protagonisti personaggi come Edward Snowden, che nel 2013 rivelò i dettagli dei programmi di sorveglianza globale della NSA; i Panama Papers, che nel 2016 hanno esposto schemi di evasione fiscale su scala internazionale; e Guccifer 2.0, un'entità collegata agli attacchi informatici che hanno colpito il Partito Democratico statunitense durante le elezioni presidenziali del 2016. Questi casi hanno messo in evidenza la portata transnazionale del fenomeno, generando effetti significativi non solo sui singoli Stati coinvolti, ma anche sulla comunità internazionale nel suo complesso. Dal punto di vista giuridico, la pubblicazione di documenti classificati pone sfide significative al diritto internazionale. Sebbene molte nazioni abbiano leggi rigorose per proteggere i documenti riservati – come il *Secrets Act* nel Regno Unito o *l'Espionage Act* negli Stati Uniti – il diritto internazionale non dispone ancora di un quadro normativo uniforme per affrontare situazioni in cui tali divulgazioni coinvolgano attori transnazionali. Questa lacuna normativa è particolarmente evidente quando i documenti vengono pubblicati attraverso piattaforme che operano in giurisdizioni diverse da quelle degli Stati interessati, complicando l'attribuzione delle responsabilità e l'applicazione delle sanzioni. A livello internazionale, il fenomeno solleva una tensione tra la necessità di proteggere la sovranità statale e quella di garantire la libertà di espressione e il diritto all'informazione. L'articolo 19 del Patto Internazionale sui Diritti Civili e Politici (ICCPR), ad esempio, tutela la libertà di espressione, ma consente limitazioni quando queste siano necessarie per proteggere la sicurezza nazionale o l'ordine pubblico. Questo equilibrio, però, è spesso difficile da raggiungere, poiché i confini tra interesse pubblico e violazione della segretezza sono spesso sottili e oggetto di interpretazioni divergenti. La pubblicazione di documenti classificati da parte di soggetti non statali evidenzia, dunque, la necessità di aggiornare il diritto internazionale per affrontare le sfide poste dall'era digitale.

In un mondo sempre più interconnesso, dove le informazioni possono attraversare confini in pochi istanti, la regolamentazione tradizionale appare inadeguata. L'assenza di un quadro normativo univoco rende ancora più urgente l'adozione di strumenti giuridici e meccanismi di cooperazione internazionale che siano in grado di bilanciare il diritto alla trasparenza con la tutela della sicurezza e della stabilità globale.

## 1.3 Conseguenze sul piano del diritto internazionale: responsabilità degli Stati, violazione della segretezza diplomatica, protezione dei whistleblower.

Nel 2010, WikiLeaks ha pubblicato un imponente archivio di documenti riservati, tra cui oltre 251.000 cablogrammi diplomatici statunitensi, molti dei quali classificati come "confidenziali" o "segreti". Questa divulgazione ha messo in discussione l'efficacia delle misure di sicurezza adottate dagli Stati per proteggere informazioni sensibili, sollevando interrogativi sulla responsabilità delle istituzioni governative nell'impedire fughe di notizie di tale portata. Dal punto di vista del diritto internazionale, la protezione delle informazioni classificate rientra nell'ambito della sovranità statale, un principio cardine che garantisce agli Stati il controllo esclusivo sulle proprie attività interne e sulle relazioni estere. La violazione di questo principio, come avvenuto nel caso WikiLeaks, ha avuto ripercussioni significative sia sul piano giuridico che su quello diplomatico. Un elemento centrale delle conseguenze legate alla pubblicazione dei documenti è la violazione della segretezza diplomatica, un principio fondamentale del diritto internazionale codificato nella Convenzione di Vienna del 1961 sulle relazioni diplomatiche. Questo trattato stabilisce che le comunicazioni tra Stati e rappresentanze diplomatiche devono essere protette e confidenziali, al fine di garantire il corretto funzionamento delle relazioni internazionali. La pubblicazione da parte di WikiLeaks di cablogrammi che rivelavano opinioni riservate, analisi strategiche e dettagli operativi sulle politiche estere di numerosi Stati ha avuto un impatto diretto sulla fiducia reciproca tra le nazioni, generando tensioni diplomatiche e compromettono la cooperazione internazionale. Ad esempio, le rivelazioni sui rapporti tra Stati Uniti e altri Paesi hanno esposto fratture nelle alleanze tradizionali, portando a una revisione delle modalità di comunicazione interna da parte di molti governi. Accanto alla violazione della segretezza diplomatica, il caso WikiLeaks ha sollevato una questione altrettanto cruciale: la protezione dei whistleblower. Gli individui che denunciano illeciti o

pratiche non etiche all'interno di istituzioni pubbliche o private svolgono un ruolo essenziale nel garantire la trasparenza e la responsabilità. Tuttavia, la loro posizione è estremamente vulnerabile, poiché spesso si trovano a subire conseguenze legali, sociali ed economiche per le loro azioni. Nel caso di WikiLeaks, Chelsea Manning, l'ex analista dell'esercito statunitense che ha fornito i documenti alla piattaforma, è stata arrestata e condannata a 35 anni di carcere (poi commutati a 7 anni dall'amministrazione Obama). Allo stesso modo, Julian Assange, fondatore di WikiLeaks, è stato accusato dagli Stati Uniti di violazione dell'Espionage Act del 1917, rischiando una pena detentiva fino a 175 anni se estradato. Questi casi evidenziano la tensione tra il diritto di denunciare abusi e le misure punitive adottate dagli Stati per salvaguardare la sicurezza nazionale. La protezione dei whistleblower è una questione che trova solo una parziale regolamentazione nel diritto internazionale. Mentre alcuni strumenti, come la Dichiarazione universale dei diritti dell'uomo e il Patto internazionale sui diritti civili e politici, riconoscono la libertà di espressione come un diritto fondamentale, essi consentono deroghe in presenza di esigenze legate alla sicurezza nazionale o all'ordine pubblico. Tuttavia, queste deroghe devono essere proporzionate e non utilizzate per reprimere il dissenso o il diritto all'informazione. Organizzazioni internazionali, come Amnesty International, hanno sottolineato l'importanza di garantire la protezione di coloro che denunciano illeciti, promuovendo la creazione di normative internazionali che tutelino i whistleblower e limitino l'abuso di leggi contro la sicurezza nazionale per perseguitarli. Il caso WikiLeaks ha evidenziato le profonde contraddizioni e tensioni che emergono nel rapporto tra diritto internazionale, sicurezza nazionale e libertà di informazione. Da un lato, gli Stati hanno il diritto e il dovere di proteggere le proprie informazioni riservate per garantire la stabilità delle relazioni internazionali e la sicurezza dei cittadini. Dall'altro lato, la trasparenza e la responsabilità sono principi fondamentali di una società democratica, che richiedono un equilibrio tra la protezione delle informazioni e il diritto del pubblico a conoscere le azioni dei governi. Questo equilibrio, tuttavia, è difficile da raggiungere, soprattutto in un contesto in cui le tecnologie digitali amplificano la portata e l'impatto delle fughe di notizie, rendendo necessaria una revisione delle normative internazionali.

## 1.4 Ruolo degli Stati Uniti e le risposte internazionali.

Gli Stati Uniti hanno adottato una posizione particolarmente rigida nei confronti di WikiLeaks, considerandola una minaccia diretta alla propria sicurezza nazionale. La pubblicazione di documenti riguardanti le guerre in Afghanistan e Iraq, con dettagli su operazioni militari, vittime civili e dinamiche interne, ha esposto aspetti delle strategie statunitensi che erano destinati a rimanere segreti. A ciò si sono aggiunti i cosiddetti "Cablegate", ovvero migliaia di cablogrammi diplomatici che hanno rivelato opinioni e analisi riservate sui rapporti con altri Paesi, mettendo in crisi non solo la fiducia tra gli Stati ma anche la reputazione degli Stati Uniti sul piano internazionale.[25] In risposta a queste divulgazioni, il Dipartimento di Giustizia degli Stati Uniti ha incriminato Julian Assange per violazione dell'Espionage Act del 1917,[26] un provvedimento storico utilizzato per perseguire chiunque divulghi informazioni considerate vitali per la sicurezza nazionale. Assange è stato accusato non solo di aver ricevuto e pubblicato documenti riservati, ma anche di aver cospirato per ottenere l'accesso a tali informazioni attraverso mezzi illeciti. La posizione statunitense, tuttavia, ha sollevato questioni controverse a livello internazionale, soprattutto per quanto riguarda la libertà di stampa e la protezione dei whistleblower. Da un lato, gli Stati Uniti hanno sottolineato che le azioni di WikiLeaks hanno messo in pericolo non solo la sicurezza del Paese ma anche la vita di individui coinvolti nelle operazioni militari e diplomatiche. Dall'altro lato, molti attivisti, giornalisti e organizzazioni internazionali per i diritti umani hanno evidenziato come la risposta americana possa rappresentare un tentativo di reprimere il diritto all'informazione e di intimidire chiunque cerchi di rivelare pratiche illecite o abusi di potere. In particolare, l'arresto di Julian Assange a Londra nel 2019, su richiesta di estradizione degli Stati Uniti, è stato visto da molti come un attacco diretto alla libertà di stampa. Organizzazioni come Amnesty International [27]hanno denunciato

---

[25]*T.Timm,* Cablegate One Year Later: How WikiLeaks Has Influenced Foreign Policy, Journalism, and the First Amendment,2011,eff.org

[26] *Espionage Act: L'Espionage Act del 1917 è una legge federale statunitense promulgata durante la Prima Guerra mondiale, volta a punire lo spionaggio e la divulgazione di informazioni sensibili sulla sicurezza nazionale. Negli anni recenti, è stato utilizzato per perseguire informatori e giornalisti, incluso Julian Assange, sollevando questioni sulla libertà di stampa e la protezione dei whistleblower."*

[27]*Annullare le accuse contro Julian Assange, 2024, amnesty.it* (Annullare le accuse contro Julian Assange, 2024) (P.L.Bellia, 2012) (d'Europa) (d'Europa; d'Europa; d'Europa; d'Europa)

le accuse contro Assange, sottolineando che la sua estradizione potrebbe avere un effetto dissuasivo su giornalisti e whistleblower in tutto il mondo. Le risposte internazionali al caso WikiLeaks hanno variato notevolmente. Alcuni governi hanno espresso solidarietà agli Stati Uniti, condividendo la preoccupazione per la compromissione della sicurezza nazionale e per i danni diplomatici causati dalla diffusione dei cablogrammi. Altri, invece, hanno criticato la rigidità americana, sottolineando che la trasparenza e la responsabilità istituzionale rappresentano valori fondamentali in una democrazia. Le reazioni della comunità internazionale riflettono così una tensione irrisolta tra la necessità di garantire la sicurezza dello Stato e il diritto del pubblico a essere informato su questioni di interesse generale. Inoltre, il caso WikiLeaks ha messo in luce il problema della regolamentazione del cyberspazio nel contesto del diritto internazionale. Sebbene gli Stati Uniti abbiano cercato di contrastare l'operato di WikiLeaks attraverso leggi nazionali come l'Espionage Act, la natura transnazionale delle piattaforme digitali e la difficoltà di applicare le giurisdizioni tradizionali hanno complicato notevolmente la questione. Le collaborazioni tra Stati, come quella tra Stati Uniti e Regno Unito per arrestare Assange, mostrano la crescente importanza della cooperazione internazionale nel contrastare le minacce informatiche e nel perseguire chi viola le leggi sulla protezione delle informazioni. Tuttavia, questa cooperazione solleva anche interrogativi sulla sovranità statale e sui limiti dell'intervento internazionale in questioni che riguardano la libertà di espressione. Oltre alle dinamiche strettamente legate alla sicurezza nazionale e alla libertà di informazione, il caso WikiLeaks ha messo in evidenza alcune problematiche strutturali relative al ruolo degli Stati Uniti come potenza egemone nel sistema internazionale. Gli Stati Uniti, essendo tra i principali promotori delle norme del diritto internazionale contemporaneo, si sono trovati in una posizione paradossale: da un lato, hanno invocato il rispetto delle leggi internazionali per giustificare la loro azione contro Julian Assange e WikiLeaks; dall'altro, sono stati accusati di utilizzare la loro influenza per imporre una visione unilaterale del concetto di sicurezza nazionale. Questo aspetto è stato particolarmente criticato da alcuni Paesi e organizzazioni internazionali, che hanno visto nell'atteggiamento statunitense un tentativo di rafforzare il controllo sulle informazioni globali e di limitare la libertà di espressione a livello transnazionale. Le accuse contro Julian Assange e la richiesta di estradizione hanno inoltre aperto un importante dibattito

sul concetto di extraterritorialità della legge. Gli Stati Uniti, attraverso l'Espionage Act, hanno cercato di perseguire un cittadino straniero per azioni compiute al di fuori del loro territorio, sollevando questioni relative alla legittimità di applicare norme nazionali a soggetti che operano in uno spazio virtuale e globalizzato.[28] Questo approccio ha portato alcuni esperti di diritto internazionale a interrogarsi sulla necessità di sviluppare un quadro normativo globale per affrontare questioni legate alla divulgazione di informazioni riservate, alla cybersicurezza e alla protezione dei whistleblower. Un ulteriore elemento di complessità riguarda la posizione ambivalente degli Stati Uniti rispetto alla libertà di stampa e alla protezione dei diritti umani. Sebbene gli Stati Uniti si siano tradizionalmente presentati come un baluardo della libertà di espressione e della democrazia, il caso WikiLeaks ha messo in discussione questa narrativa. La decisione di perseguire Assange, anziché concentrarsi sulle vulnerabilità interne che hanno permesso la fuga di documenti, è stata interpretata da molti come una strategia per scoraggiare future fughe di informazioni, piuttosto che come un reale tentativo di risolvere i problemi strutturali legati alla gestione dei dati classificati. Questo ha generato tensioni con organizzazioni non governative e governi che considerano la trasparenza un valore fondamentale per la democrazia. Un altro aspetto che merita attenzione è il ruolo delle alleanze internazionali nel supportare gli Stati Uniti nel perseguire Assange e nel mitigare le conseguenze diplomatiche delle rivelazioni di WikiLeaks. Paesi come il Regno Unito hanno collaborato strettamente con gli Stati Uniti, arrestando Assange e detenendolo per anni nell'ambasciata ecuadoriana a Londra. Al tempo stesso, altre nazioni, come l'Ecuador, hanno assunto posizioni più critiche, concedendo asilo politico ad Assange nel 2012 e sottolineando la necessità di proteggere chi denuncia abusi di potere.[29] Sul piano del diritto internazionale, il caso ha evidenziato un vuoto normativo riguardo alla regolamentazione dello spazio digitale e al trattamento dei whistleblower. Non esiste, infatti, un consenso internazionale sulla protezione di chi denuncia illeciti attraverso piattaforme globali, né un quadro chiaro che definisca i limiti tra libertà di espressione e sicurezza nazionale. Questo ha portato

[28] *P.L. Bellia, WikiLeaks and the Institutional Framework for National Security Disclosures, The Yale Law Journal, 2012*

[29] Risoluzione 2571, La detenzione e la condanna di Julian Assange e i loro effetti sui diritti umani dell'Assemblea Parlamentare del Consiglio d'Europa,

a una crescente pressione per sviluppare trattati o linee guida internazionali che possano affrontare queste sfide in maniera equilibrata, garantendo che i diritti fondamentali siano rispettati anche in un contesto altamente politicizzato. Il caso WikiLeaks ha inoltre spinto molti Stati, tra cui gli stessi Stati Uniti, a rivedere le proprie strategie di sicurezza digitale e di gestione delle informazioni riservate. Dopo le rivelazioni, il governo statunitense ha implementato misure più rigorose per limitare l'accesso a dati classificati, rafforzare i sistemi informatici e identificare potenziali minacce interne. Tuttavia, queste misure hanno sollevato interrogativi sulla sorveglianza dei dipendenti pubblici e sull'erosione della privacy anche all'interno delle stesse istituzioni governative. Infine, le implicazioni di WikiLeaks hanno avuto un impatto duraturo sulla diplomazia internazionale, spingendo molti governi, tra i quali quello italiano, a privilegiare canali di comunicazione più sicuri e a ridurre l'uso di mezzi digitali per trasmettere informazioni sensibili.[30] Questo fenomeno, sottolinea come il cyberspionaggio e la divulgazione di informazioni riservate abbiano trasformato profondamente il modo in cui gli Stati operano nel sistema internazionale. Il ruolo degli Stati Uniti nel caso WikiLeaks evidenzia il difficile equilibrio tra la necessità di proteggere la sicurezza nazionale e l'importanza di garantire la libertà di informazione. Le risposte statunitensi, caratterizzate da azioni legali e richieste di estradizione, hanno avuto un forte impatto sulla comunità internazionale, alimentando un dibattito che va ben oltre il caso specifico. [31] Il caso mette in luce la difficoltà di applicare il diritto nazionale a entità come WikiLeaks, che operano in un ambiente globale e decentralizzato. Mentre i media tradizionali, con una presenza significativa negli Stati Uniti, sono soggetti alla giurisdizione americana, WikiLeaks, privo di una presenza fisica nel territorio statunitense e in grado di utilizzare infrastrutture distribuite in tutto il mondo, sfida la capacità del governo di imporre vincoli preventivi o sanzioni penali. Questo solleva importanti questioni di diritto internazionale e di regolamentazione del cyberspazio, richiedendo un ripensamento del quadro normativo esistente per affrontare in modo adeguato la divulgazione di informazioni di sicurezza nazionale in un mondo digitale.

[30] *Frattini, Le nuove forme della diplomazia, "Dossier Lazio" intervista al ministro degli Affari Esteri, 2011*
[31] *Analisi ISP sull'estradizione di Assange e il cyberspionaggio*, *ISPI Online,* 2024

## 2 Datagate: spionaggio tra alleati e diritto internazionale

Il caso *Datagate* rappresenta una delle più significative rivelazioni nella storia della sorveglianza di massa e del cyberspionaggio, avvenuta nel 2013. Questa vicenda ha messo in luce i complessi intrecci tra sicurezza nazionale, protezione dei diritti individuali e responsabilità degli Stati nel contesto globale. Al centro del caso vi è Edward Snowden, ex consulente della National Security Agency (NSA) statunitense, che ha divulgato una vasta quantità di documenti riservati relativi ai programmi di sorveglianza condotti dagli Stati Uniti, molti dei quali in collaborazione con altri governi. Tali rivelazioni hanno sollevato questioni cruciali nel diritto internazionale, legate alla tutela della privacy, alla sicurezza nazionale e alla sovranità degli Stati. Nel giugno 2013, Edward Snowden ha reso pubblici, attraverso i media internazionali *The Guardian*, *The Washington Post** e altri, documenti riservati che dimostravano l'esistenza di programmi di sorveglianza di massa condotti dalla NSA, tra cui il famoso programma *PRISM.* Attraverso *PRISM*, la NSA poteva accedere a dati personali di milioni di individui, raccolti da grandi aziende tecnologiche come Google, Facebook, Microsoft e Apple. Questi programmi erano giustificati dall'esigenza di prevenire minacce terroristiche, in particolare dopo gli attacchi dell'11 settembre 2001, ma il loro impatto si estendeva ben oltre le finalità dichiarate. Le rivelazioni includevano anche dettagli sulla raccolta massiva di dati telefonici dove l'NSA aveva accesso ai metadati delle telefonate effettuate da milioni di cittadini statunitensi, indipendentemente dal loro coinvolgimento in attività sospette, sorveglianza internazionale: programmi come XKeyscore permettevano di monitorare le attività online di individui in tutto il mondo ed intercettazioni di leader stranieri: tra cui Angela Merkel, allora cancelliera tedesca, dimostrando che la sorveglianza statunitense non si limitava a potenziali minacce terroristiche, ma si estendeva anche agli alleati. Il caso Datagate ha avuto conseguenze di portata globale, poiché ha rivelato come la sorveglianza condotta dagli Stati Uniti si estendesse ben oltre i propri confini, coinvolgendo cittadini, governi e istituzioni di altri Paesi. Molti Stati, soprattutto in Europa, hanno reagito con preoccupazione e indignazione, considerandolo una violazione della loro sovranità e del diritto alla riservatezza. Il caso ha sollevato interrogativi fondamentali sulla compatibilità di tali pratiche con il diritto internazionale, in particolare con il rispetto della privacy sancito dall'articolo 17 del Patto Internazionale sui Diritti Civili e Politici

(ICCPR). Al contempo, il Datagate ha evidenziato le lacune normative a livello internazionale per quanto riguarda la regolamentazione della sorveglianza transnazionale. Sebbene alcune convenzioni internazionali e regionali, come la Convenzione europea dei diritti dell'uomo (art. 8), garantiscano la protezione della privacy, esse non prevedono strumenti adeguati ad affrontare le implicazioni del cyberspionaggio su larga scala. Il governo statunitense ha giustificato i programmi di sorveglianza come strumenti indispensabili per garantire la sicurezza nazionale e prevenire attacchi terroristici. Tuttavia, le rivelazioni di Snowden hanno dimostrato come tali programmi fossero spesso utilizzati in modo sproporzionato, violando i diritti fondamentali dei cittadini e compromettendo la fiducia tra gli Stati. In risposta alle critiche, gli Stati Uniti hanno introdotto alcune riforme, come il *Freedom Act del 2015*, che ha posto limiti alla raccolta indiscriminata di dati telefonici. Nonostante ciò, le critiche internazionali sono rimaste forti, poiché le riforme non hanno affrontato pienamente il problema della sorveglianza transnazionale. La figura di Edward Snowden è stata al centro del dibattito globale. Per molti, egli è un *whistleblower*, che ha avuto il coraggio di esporre abusi di potere a beneficio dell'interesse pubblico. Snowden ha dichiarato di aver agito per difendere i diritti fondamentali delle persone, in particolare il diritto alla privacy, che riteneva gravemente compromesso. Tuttavia, per il governo statunitense, Snowden è un "traditore", accusato di aver violato *l'Espionage Act del 1917* e di aver messo in pericolo la sicurezza nazionale attraverso la divulgazione di informazioni riservate. Snowden ha ottenuto asilo politico in Russia nel 2013, dopo essere fuggito dagli Stati Uniti, e da allora è rimasto lì, nonostante le richieste di estradizione degli Stati Uniti. Il suo caso ha sollevato una discussione globale sulla protezione dei whistleblower, evidenziando come molti Stati non dispongano di normative adeguate a garantire la sicurezza di chi denuncia illeciti o abusi di potere. Il Datagate ha avuto un impatto duraturo sul diritto internazionale e sulle relazioni tra gli Stati. Da un lato, ha messo in evidenza l'urgenza di sviluppare norme internazionali che regolino la sorveglianza e il trattamento dei dati personali. Dall'altro, ha alimentato un clima di sfiducia tra gli Stati, soprattutto tra gli Stati Uniti e i loro alleati europei, come dimostrato dal caso delle intercettazioni della cancelliera Merkel. Inoltre, il caso ha spinto l'Unione Europea ad accelerare l'adozione del Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore nel 2018, con l'obiettivo di

rafforzare la tutela dei dati personali e di imporre obblighi stringenti alle aziende e ai governi che trattano tali dati. Il Datagate ha segnato un punto di svolta nel modo in cui la società percepisce il rapporto tra sicurezza e privacy nell'era digitale. Ha sollevato interrogativi fondamentali sulla legittimità della sorveglianza di massa e sulla capacità degli Stati di bilanciare la protezione della sicurezza nazionale con il rispetto dei diritti fondamentali. Allo stesso tempo, ha evidenziato la necessità di una maggiore trasparenza e di una regolamentazione internazionale più efficace per affrontare le sfide poste dalla digitalizzazione e dall'interconnessione globale.

## 2.1 Il ruolo della NSA nel Datagate

La National Security Agency (NSA) ha svolto un ruolo centrale nel caso Datagate, incarnando la massima espressione delle operazioni di sorveglianza globale e del cyberspionaggio condotto dagli Stati Uniti. Fondata nel 1952 con l'obiettivo di raccogliere e analizzare comunicazioni elettroniche a scopo di sicurezza nazionale, la NSA ha progressivamente ampliato la sua portata con l'evoluzione delle tecnologie digitali, acquisendo capacità operative senza precedenti. Le rivelazioni di Edward Snowden, avvenute nel 2013, hanno svelato come questa agenzia abbia implementato una rete globale di sorveglianza, giustificandola come necessaria per combattere il terrorismo e proteggere gli interessi statunitensi, ma sollevando profonde questioni etiche, legali e politiche. A seguito degli attentati dell'11 settembre 2001, la NSA ha visto espandere significativamente il proprio mandato, soprattutto grazie al *Patriot Act*, che ha conferito all'agenzia poteri straordinari di sorveglianza, anche senza l'obbligo di autorizzazioni specifiche da parte del sistema giudiziario. Questo quadro normativo ha permesso alla NSA di sviluppare programmi tecnologici sofisticati per raccogliere dati non solo su potenziali minacce terroristiche, ma anche su cittadini ordinari, aziende private e leader politici, coinvolgendo tanto il contesto nazionale quanto quello internazionale. Tuttavia, le rivelazioni di Snowden hanno portato alla luce un modello di sorveglianza che andava ben oltre quanto pubblicamente dichiarato, sollevando interrogativi cruciali sui limiti della sicurezza nazionale e il rispetto dei diritti fondamentali. Le operazioni della NSA erano condotte attraverso una rete complessa di programmi tecnologici, ognuno

progettato per intercettare dati e comunicazioni su scala globale. Tra i più rilevanti, spiccano: PRISM, che consentiva l'accesso diretto ai dati raccolti da grandi aziende tecnologiche statunitensi come Google, Facebook e Microsoft. Attraverso PRISM, la NSA acquisiva e-mail, conversazioni vocali, messaggi e documenti degli utenti, spesso senza il loro consenso, utilizzando autorizzazioni legali vaghe e permissive. *XKeyscore*: uno strumento avanzato che permetteva di analizzare le attività online in tempo reale, monitorando ricerche web, e-mail e cronologie di navigazione. Questo programma non era limitato a sospetti terroristi, ma raccoglieva dati di milioni di utenti in tutto il mondo. Upstream: un sistema che intercettava comunicazioni direttamente dalle infrastrutture globali di telecomunicazione, come cavi in fibra ottica, grazie alla collaborazione di provider di rete e aziende tecnologiche. Intercettazioni di leader politici: che hanno rivelato la sorveglianza di capi di Stato stranieri, tra cui Angela Merkel, cancelliera tedesca. Questo aspetto ha generato tensioni diplomatiche significative tra gli Stati Uniti e i loro alleati. Raccolta di metadati telefonici, che permetteva alla NSA di tracciare numeri di telefono, durata delle chiamate e frequenza delle comunicazioni, anche in assenza di un nesso diretto con attività criminali. Questi programmi dimostrano come la NSA abbia costruito una rete capillare di controllo globale, capace di raccogliere informazioni su scala senza precedenti, grazie anche alla cooperazione con altre agenzie e governi. Le operazioni della NSA non si limitavano agli Stati Uniti, ma si estendevano su scala internazionale attraverso collaborazioni con altre agenzie di intelligence. La rete *Five Eyes*, composta da Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda, rappresenta un esempio emblematico di tale cooperazione. Questi Paesi hanno condiviso infrastrutture, informazioni e risorse per ampliare le capacità di sorveglianza transnazionale. Tuttavia, questa cooperazione ha sollevato interrogativi sul rispetto della sovranità degli Stati coinvolti, soprattutto quando le operazioni riguardavano cittadini stranieri o governi alleati. Le attività della NSA, benché giustificate con l'obiettivo di garantire la sicurezza nazionale, hanno sollevato gravi preoccupazioni sul piano etico e giuridico. Le rivelazioni di Snowden hanno evidenziato una sistematica violazione della privacy, sia a livello individuale che collettivo. Molte delle operazioni della NSA erano coperte da autorizzazioni legali interne, ma queste normative sono state criticate per la loro vaghezza e per l'assenza di meccanismi di controllo democratico. A livello

internazionale, la sorveglianza condotta su leader politici e cittadini stranieri ha generato accuse di violazione della sovranità statale e del diritto alla riservatezza, sancito da strumenti come l'articolo 17 del Patto Internazionale sui Diritti Civili e Politici (ICCPR). Il caso NSA ha sollevato inoltre interrogativi sulla proporzionalità delle misure di sorveglianza rispetto agli obiettivi dichiarati. Se da un lato le autorità statunitensi hanno sostenuto che tali operazioni erano essenziali per prevenire attacchi terroristici, dall'altro lato molte analisi indipendenti hanno evidenziato come la sorveglianza di massa abbia avuto un impatto limitato sull'effettiva prevenzione di minacce, compromettendo invece la fiducia tra i cittadini e le istituzioni. Le rivelazioni di Snowden hanno avuto un impatto duraturo sia sugli Stati Uniti che sul panorama internazionale. Negli Stati Uniti, il Freedom Act del 2015 ha introdotto alcune limitazioni alla raccolta indiscriminata di dati telefonici, trasferendo il controllo dei metadati a operatori privati e riducendo i poteri della NSA in alcuni ambiti. Tuttavia, molte delle critiche fondamentali alla sorveglianza di massa non sono state affrontate, lasciando aperto il dibattito su come bilanciare sicurezza e diritti fondamentali. A livello globale, il caso ha spinto diversi Paesi, soprattutto in Europa, a rafforzare le proprie normative sulla protezione dei dati personali.

## 2.2 Impatti sul principio di fiducia e cooperazione tra Stati (spionaggio tra alleati).

Il caso Datagate ha messo in luce come le attività di sorveglianza e cyberspionaggio possano compromettere la fiducia reciproca tra Stati, anche tra quelli uniti da solidi rapporti di alleanza. Il principio di fiducia e cooperazione è un pilastro fondamentale delle relazioni internazionali, particolarmente nel contesto di organizzazioni sovranazionali come la NATO e l'Unione Europea, dove la condivisione di informazioni sensibili è essenziale per garantire la sicurezza collettiva. Tuttavia, le rivelazioni di Edward Snowden hanno dimostrato come le operazioni di intelligence statunitensi non si limitassero al contrasto di minacce esterne, ma coinvolgessero anche governi e leader politici di Paesi alleati.

L'intercettazione delle comunicazioni di figure di spicco come Angela Merkel[32] ha sollevato interrogativi sulla lealtà tra Stati e sul rispetto degli obblighi internazionali. Lo spionaggio tra alleati mette in discussione il concetto stesso di

[32] *Stefani.S, Il caso Snowden e le conseguenze diplomatiche del Datagate, Treccani.it, 2013*

cooperazione internazionale, sollevando il dubbio che le informazioni condivise possano essere sfruttate per finalità diverse da quelle dichiarate. Questo ha portato a un clima di sospetto reciproco, con conseguenze dirette sulla diplomazia e sui rapporti tra gli Stati, nonché sulla revisione dei meccanismi di scambio di dati tra agenzie di intelligence. [33]

Dal punto di vista giuridico, il diritto internazionale non disciplina espressamente le attività di spionaggio tra Stati alleati, lasciando un vuoto normativo che rende difficile perseguire tali condotte. Tuttavia, vi sono principi generali che risultano compromessi da queste pratiche, in particolare il principio di sovranità statale e il principio di non ingerenza negli affari interni. La Carta delle Nazioni Unite (art. 2, par. 4) stabilisce il divieto di minaccia o uso della forza contro l'integrità territoriale e l'indipendenza politica di qualsiasi Stato, e sebbene lo spionaggio non costituisca un atto di forza in senso stretto, può essere considerato una forma di ingerenza indebita, specialmente quando viola accordi di collaborazione e di fiducia reciproca tra Stati.

Inoltre, la protezione della privacy è garantita da trattati internazionali come il Patto Internazionale sui Diritti Civili e Politici (ICCPR)e la Convenzione Europea dei Diritti dell'Uomo (CEDU), entrambi strumenti che possono essere richiamati per contestare attività di sorveglianza indiscriminata da parte dei servizi di intelligence. Il Datagate ha dimostrato come tali pratiche abbiano violato la privacy non solo dei leader politici, ma anche di cittadini comuni, creando una frattura tra gli Stati coinvolti e mettendo in discussione la legittimità delle operazioni di intelligence condotte dagli Stati Uniti. [34]

Uno degli impatti più evidenti dello spionaggio tra alleati è la progressiva erosione del principio di cooperazione internazionale[35]. Questo principio, riconosciuto in numerosi trattati e dichiarazioni multilaterali, come la Dichiarazione sulle Relazioni Amichevoli del 1970[36], stabilisce che gli Stati devono cooperare in

[33] *Consiglio d'Europa,* Risoluzione sulla sorveglianza di massa dell'NSA, 2015
[34] *European Parliament,* NSA snooping: MEPs table proposals to protect EU citizens' privacy, 2014
[35] A.Ligustro, Principio pacifista e uso della forza nel diritto internazionale contemporaneo, 2023, Convegno DPCE Pescara (Unite, 1970)
[36] *Risoluzione dell'assemblea genrale delle Nazioni Unite, Dichiarazione relativa ai principi di diritto intenrazionale, concernenti le r* (N.Ronzitti, 2013) (Tutela della Sicurezza Pubblica vs Tutela della Privacy: un bilanciamento necessario, 2020)*elazioni amichevoli e la cooperazione tra gli stati in conformità con la carta delle Nazioni Unite, 1970*

buona fede per il mantenimento della pace e sicurezza internazionale. Tuttavia, lo scandalo Datagate ha dimostrato che persino tra partner strategici vi è la costante ricerca di un vantaggio informativo a scapito della trasparenza e del rispetto reciproco. La rivelazione di queste pratiche ha portato a un raffreddamento delle relazioni transatlantiche e a una revisione delle modalità di scambio di informazioni tra le agenzie di intelligence, con alcuni Paesi che hanno introdotto limitazioni nella cooperazione con gli Stati Uniti. A seguito delle rivelazioni di Snowden, diversi Stati hanno adottato misure per proteggersi da future attività di spionaggio. Tra queste figurano:

- Riforme legislative volte a rafforzare la protezione dei dati personali, culminate nell'adozione del Regolamento Generale sulla Protezione dei Dati (GDPR) da parte dell'Unione Europea.

- Richieste di chiarimenti ufficiali e azioni diplomatiche per ottenere maggiore trasparenza nelle attività di sorveglianza statunitense.

- Rafforzamento dei protocolli di sicurezza informatica per prevenire infiltrazioni nei sistemi governativi.

- Rinegoziazione degli accordi di condivisione delle informazioni tra Stati alleati, con l'obiettivo di stabilire limiti più stringenti all'uso delle informazioni scambiate.

Nonostante le reazioni internazionali e la condanna pubblica, il Datagate ha evidenziato i limiti del diritto internazionale nel contrastare efficacemente lo spionaggio tra Stati alleati. La mancanza di un trattato specifico che vieti esplicitamente tali attività ha fatto sì che le azioni intraprese rimanessero principalmente nel campo della diplomazia, piuttosto che in quello della sanzione giuridica.[37] Infine, il Datagate ha acceso un dibattito più ampio sul bilanciamento tra sicurezza e privacy.[38] Da un lato, gli Stati Uniti hanno giustificato le loro attività di sorveglianza come strumenti necessari per la lotta al terrorismo e la protezione della sicurezza nazionale. Dall'altro, molti governi e organizzazioni internazionali hanno sottolineato che la sicurezza non può essere perseguita a

[37] *N.Ronzitti, Datagate le regole dello spionaggio, 2013, formiche.net*
[38] *Tutela della Sicurezza Pubblica vs Tutela della Privacy: un bilanciamento necessario, 2020,diritto.it*

scapito dei diritti fondamentali, evidenziando come la raccolta indiscriminata di dati rappresenti una minaccia alla democrazia e alla libertà individuale.

## 2.3 Riflessioni sulle implicazioni per i diritti umani, in particolare il diritto alla privacy (art. 17 ICCPR).

Il caso Datagate ha sollevato questioni di primaria importanza nell'ambito del diritto internazionale, evidenziando le criticità connesse alla tutela della privacy nel contesto della sorveglianza di massa. [39] Il diritto alla privacy rappresenta un diritto umano fondamentale, sancito dall'articolo 17 del Patto Internazionale sui Diritti Civili e Politici (ICCPR), il quale vieta qualsiasi interferenza arbitraria o illegale nella vita privata, nella corrispondenza e nella reputazione di un individuo. Tuttavia, le pratiche di sorveglianza globale rivelate da Edward Snowden hanno evidenziato la difficoltà di garantire una protezione effettiva di tale diritto, determinando un acceso dibattito sulla sua compatibilità con le esigenze di sicurezza nazionale. L'articolo 17 dell'ICCPR sancisce che "Nessun individuo potrà essere soggetto a interferenze arbitrarie o illegali nella sua vita privata, famiglia, domicilio o corrispondenza" e che "Ogni individuo ha diritto alla protezione della legge contro tali interferenze o lesioni". Tale disposizione impone agli Stati l'obbligo di adottare misure adeguate volte a garantire il rispetto della privacy, assicurando che eventuali limitazioni siano conformi ai principi di legalità, necessità e proporzionalità, imprescindibili nel diritto internazionale per valutare la legittimità di eventuali restrizioni ai diritti fondamentali. Le rivelazioni emerse dal Datagate hanno dimostrato come programmi di sorveglianza, quali PRISM, abbiano operato al di fuori di controlli giuridici trasparenti e con un impatto globale, incidendo anche sulla sovranità di Stati terzi. In questo senso, la sorveglianza di massa può essere qualificata come una violazione non solo dell'art. 17 ICCPR, ma anche del principio di non ingerenza negli affari interni degli Stati, espressamente sancito dall'articolo 2(7) della Carta delle Nazioni Unite. Le principali corti internazionali hanno più volte ribadito l'importanza della tutela della privacy nell'ordinamento giuridic (The protection of privacy and personal data on the Internet and online media, 2011) (Unite C. p.) (Privacy Rights

[39] *The protection of privacy and personal data on the Internet and online media, assembly.coe.int, 2011*

in the Digital Age, 2013) (F.Schifilliti, 2023) (Cistenrino, 2022) (V.Poitevin, 2024)o internazionale. La Corte Europea dei Diritti dell'Uomo (CEDU) ha affrontato il tema in diverse pronunce, tra cui la sentenza Zakharov c. Russia (2015), nella quale ha dichiarato che le legislazioni che consentono la sorveglianza segreta devono prevedere garanzie adeguate contro abusi e arbitrarietà. Il Comitato per i Diritti Umani delle Nazioni Unite, organo preposto al monitoraggio dell'ICCPR, ha espresso preoccupazioni analoghe, sottolineando che le attività di intelligence devono essere compatibili con il principio di proporzionalità e sottoposte a controllo giurisdizionale indipendente. Inoltre, il caso Schrems I (2015) e Schrems II (2020) , deciso dalla Corte di Giustizia dell'Unione Europea (CGUE), ha avuto un impatto significativo sulla regolamentazione internazionale della protezione dei dati personali, evidenziando l'inadeguatezza delle garanzie offerte dal regime giuridico statunitense in materia di trasferimento di dati personali. A seguito dello scandalo Datagate, la comunità internazionale ha avviato iniziative volte a rafforzare la tutela del diritto alla privacy nel contesto digitale.  L'Unione Europea ha adottato il Regolamento Generale sulla Protezione dei Dati (GDPR), il quale stabilisce standard rigorosi per il trattamento dei dati personali, imponendo limiti più stringenti sulla raccolta e l'uso delle informazioni da parte di soggetti pubblici e privati. Tuttavia, a livello universale, l'assenza di uno strumento giuridico vincolante che disciplini in modo dettagliato la sorveglianza di massa costituisce una lacuna significativa. Anche negli Stati Uniti, pur essendo stato introdotto il USA Freedom Act (2015) per limitare alcuni poteri della NSA, il quadro normativo vigente continua a sollevare perplessità in merito alla compatibilità con gli standard internazionali in materia di diritti umani. L'assenza di una regolamentazione chiara e vincolante a livello globale favorisce l'adozione di pratiche di sorveglianza poco trasparenti, minando il principio di legalità e il diritto alla protezione effettiva sancito dall'ICCPR. Il Datagate ha rappresentato un punto di svolta nella discussione internazionale sulla protezione della privacy, evidenziando la necessità di un quadro giuridico più solido e armonizzato. Sebbene alcune iniziative normative abbiano cercato di limitare gli effetti della sorveglianza indiscriminata, permane la necessità di un maggiore coordinamento tra gli Stati e gli organismi internazionali per garantire che le attività di intelligence siano conformi ai principi fondamentali del diritto

internazionale. Riflessioni sulle implicazioni per i diritti umani internazionali, in particolare il diritto alla privacy (art. 17 ICCPR). [4041]

## 3 Cyberspionaggio e il conflitto russo-ucraino

Il conflitto tra Russia e Ucraina rappresenta un caso emblematico dell'evoluzione della guerra moderna, in cui le operazioni cibernetiche sono diventate uno strumento strategico di primaria importanza. [4243] Il cyberspionaggio, in particolare, si è rivelato un elemento cruciale nelle dinamiche della guerra, permettendo agli attori coinvolti di raccogliere informazioni sensibili, condurre azioni di sabotaggio e influenzare il panorama politico e militare attraverso operazioni informatiche su larga scala. Fin dalle prime fasi del conflitto, la Russia ha impiegato strumenti di spionaggio informatico per monitorare le comunicazioni ucraine, intercettare dati strategici e destabilizzare le infrastrutture critiche del Paese. L'uso di malware sofisticati, attacchi alle reti governative e intrusioni nei sistemi di difesa ha consentito di ottenere un vantaggio informativo significativo. Tali operazioni non si sono limitate alle istituzioni ucraine, ma hanno coinvolto anche attori internazionali, evidenziando la dimensione transnazionale del cyberspionaggio. D'altro canto, l'Ucraina ha sviluppato nel tempo una crescente capacità di difesa cibernetica, anche grazie al supporto di alleati occidentali e aziende private specializzate in sicurezza informatica. La cooperazione tra governi e settore privato ha permesso di mitigare parte delle minacce, adottando strategie di protezione avanzate e rafforzando la resilienza delle infrastrutture digitali. Inoltre, il conflitto ha visto emergere il ruolo sempre più attivo di gruppi di hacker, sia filorussi che filo-ucraini, i quali hanno contribuito a rendere il cyberspazio un vero e proprio campo di battaglia parallelo. Il caso russo-ucraino dimostra come il cyberspionaggio non sia più un fenomeno isolato, ma un aspetto integrato della guerra ibrida, in grado di influenzare l'andamento delle ostilità e le relazioni geopolitiche su scala globale. L'invasione

[40] *Commento Generale n. 16 del Comitato per i Diritti Umani delle Nazioni Unite, refworld.org,*

[41] *Privacy Rights in the Digital Age, 2013, aclu.org,*

[42] *F.Schifilliti, Operazioni di cyber spionaggio nel conflitto tra Russia e Ucraina, 2023, icttsecuritymagazine.com,*

[43] *S.Cistenrino, Un nuovo uso della forza: la cyberwar nella guerra russo-ucraina, 2022, scienzainrete.it,*

russa dell'Ucraina, avviata nel febbraio 2022, ha segnato un punto di svolta nella concezione moderna dei conflitti, evidenziando come la dimensione cibernetica sia divenuta un pilastro strategico delle operazioni belliche. In questo contesto, il cyberspionaggio si è rivelato uno strumento essenziale per l'acquisizione di informazioni sensibili, la manipolazione dell'opinione pubblica e la destabilizzazione delle infrastrutture critiche. Gli attacchi informatici, infatti, hanno accompagnato e talvolta anticipato le offensive militari convenzionali, dimostrando come la guerra nel cyberspazio e quella sul terreno siano oggi strettamente interconnesse. La Russia ha tradizionalmente investito in capacità avanzate di cyberspionaggio, utilizzando attori statali e gruppi affiliati per condurre operazioni su vasta scala. Nel contesto del conflitto ucraino, tali attività hanno avuto diversi obiettivi. Da un lato, il governo russo ha puntato alla raccolta di informazioni su strategie militari, piani di difesa e comunicazioni governative ucraine, facilitando così le operazioni sul campo. Dall'altro, ha sfruttato il cyberspionaggio per influenzare l'opinione pubblica, sia a livello interno che internazionale, attraverso la diffusione di propaganda e disinformazione. Uno degli strumenti principali utilizzati per il cyberspionaggio è stato il malware, progettato per infiltrarsi nei sistemi informatici di istituzioni governative, forze armate e infrastrutture critiche. Alcuni esempi significativi includono il malware *Industroyer*, impiegato per attaccare la rete elettrica ucraina, e il più recente *HermeticWiper*, un software malevolo progettato per cancellare dati e paralizzare i sistemi informatici bersaglio. Le campagne di phishing mirate hanno rappresentato un ulteriore vettore d'attacco, permettendo agli hacker russi di compromettere account di funzionari ucraini e accedere a documenti riservati. Non meno rilevante è stata l'attività di spionaggio condotta nei confronti di alleati occidentali dell'Ucraina, inclusi governi, istituzioni diplomatiche e aziende private coinvolte nella fornitura di armamenti o nella cybersicurezza. Gruppi notoriamente legati ai servizi segreti russi, come APT28 (Fancy Bear) e APT29 (Cozy Bear), hanno condotto operazioni di infiltrazione ai danni di paesi membri della NATO, nel tentativo di monitorare il supporto militare fornito a Kiev e raccogliere dati strategici per le operazioni russe. Sin dal 2014, con l'annessione della Crimea da parte della Russia, l'Ucraina ha progressivamente rafforzato le proprie capacità di difesa cibernetica, adottando misure di protezione avanzate per contrastare il cyberspionaggio russo. Tuttavia, l'intensità e la sofisticazione degli

attacchi registrati nel 2022 e negli anni successivi hanno reso necessario un maggiore coordinamento con partner internazionali, tra cui Unione Europea, Stati Uniti e aziende leader nel settore della cybersicurezza. L'assistenza fornita da società come Microsoft e Google ha giocato un ruolo cruciale nel rilevamento e nella neutralizzazione di minacce informatiche. Attraverso l'impiego di tecnologie basate sull'intelligenza artificiale e sistemi di monitoraggio avanzati, l'Ucraina è riuscita a mitigare gli effetti di numerosi attacchi. Inoltre, l'intervento di organizzazioni governative occidentali, come l'Agenzia per la Cybersicurezza e la Sicurezza delle Infrastrutture (CISA) statunitense, ha permesso di sviluppare strategie di risposta più efficaci. Un elemento chiave nella difesa ucraina è stato il coinvolgimento della comunità hacker filo-ucraina, tra cui il collettivo IT Army of Ukraine, composto da volontari provenienti da tutto il mondo. Questo gruppo ha condotto operazioni di controspionaggio e attacchi informatici contro obiettivi russi, contribuendo a danneggiare infrastrutture digitali e piattaforme di comunicazione del Cremlino. Il conflitto russo-ucraino ha reso evidente come il cyberspionaggio non sia più un fenomeno isolato o circoscritto alle fasi preliminari di una guerra, ma un elemento costante e strategico nel quadro della guerra ibrida. L'uso combinato di operazioni militari convenzionali e attacchi informatici ha introdotto una nuova dimensione nel diritto internazionale, sollevando interrogativi sulla responsabilità degli Stati, sulla legittimità delle operazioni cibernetiche e sulla necessità di un quadro normativo più chiaro per affrontare tali minacce.

## 3.1 L'uso del cyberspionaggio come strumento di guerra ibrida.

Il conflitto russo-ucraino rappresenta un caso paradigmatico dell'evoluzione della guerra ibrida, in cui il cyberspionaggio si configura come uno strumento strategico essenziale per il conseguimento di obiettivi politici e militari. Nel contesto della guerra moderna, la distinzione tra guerra convenzionale e operazioni cibernetiche è divenuta sempre più labile, evidenziando come il cyberspazio sia ormai un vero e proprio teatro di scontro in grado di influenzare significativamente le dinamiche del conflitto. L'impiego del cyberspionaggio da parte della Russia nei confronti dell'Ucraina ha dimostrato la crescente rilevanza delle operazioni digitali nella conduzione della guerra, con finalità che spaziano dalla raccolta di informazioni sensibili alla disinformazione e alla

destabilizzazione delle infrastrutture critiche. Il concetto di guerra ibrida fa riferimento a una combinazione di strumenti convenzionali e non convenzionali, militari e non militari, utilizzati in modo coordinato per ottenere un vantaggio strategico sull'avversario. Tra questi strumenti, il cyberspionaggio riveste un ruolo di primaria importanza, poiché consente di condurre operazioni di intelligence mirate, senza la necessità di un coinvolgimento diretto delle forze armate sul campo. Nel caso del conflitto russo-ucraino, l'impiego del cyberspionaggio è stato funzionale alla raccolta di informazioni sui piani militari ucraini, sulle comunicazioni governative e sulla logistica delle forze armate. Le intrusioni nei sistemi informatici di Kiev hanno permesso agli attori russi di monitorare in tempo reale le strategie difensive dell'Ucraina, migliorando l'efficacia delle operazioni militari sul terreno. Parallelamente, le campagne di spionaggio hanno colpito anche gli alleati occidentali dell'Ucraina, nel tentativo di ottenere dati riservati sulle forniture di armi e sul supporto strategico offerto dai paesi membri della NATO. Uno degli strumenti principali utilizzati per il cyberspionaggio è stato il malware, impiegato per infiltrarsi nei sistemi informatici di istituzioni governative, aziende e infrastrutture critiche. In particolare, gruppi di hacker affiliati ai servizi segreti russi che hanno condotto attacchi mirati contro enti pubblici e privati, utilizzando tecniche avanzate di phishing e exploit zero-day per compromettere i sistemi informatici. Un aspetto fondamentale del cyberspionaggio nel quadro della guerra ibrida riguarda il suo impatto sulle infrastrutture critiche. Nel caso dell'Ucraina, gli attacchi informatici hanno mirato a paralizzare settori chiave come l'energia, le telecomunicazioni e i trasporti, con l'obiettivo di indebolire la capacità di resistenza del paese. Già nel 2015 e nel 2016, prima dell'inizio dell'invasione su larga scala, la Russia aveva testato la sua capacità di attacco cibernetico contro l'Ucraina, causando blackout energetici attraverso l'uso del malware *Industroyer*. Con lo scoppio del conflitto nel 2022, questi attacchi si sono intensificati, colpendo reti elettriche, provider di servizi internet e infrastrutture di comunicazione governativa. Un esempio emblematico è stato l'attacco a *Viasat* un operatore di comunicazioni satellitari che fornisce servizi di connettività all'Ucraina, il cui sabotaggio ha compromesso le comunicazioni militari e civili nelle prime fasi dell'invasione russa. Questi attacchi informatici non solo hanno avuto un impatto diretto sulle operazioni militari e sulla popolazione civile, ma hanno anche evidenziato la vulnerabilità

delle infrastrutture critiche in un contesto di guerra ibrida. La capacità di un attore statale di infiltrarsi nei sistemi di un avversario e comprometterne il funzionamento rappresenta oggi una delle minacce più rilevanti per la sicurezza nazionale e internazionale. Oltre alla raccolta di informazioni e al sabotaggio delle infrastrutture, il cyberspionaggio è stato utilizzato come leva per condurre operazioni di disinformazione e guerra psicologica. Attraverso l'uso coordinato di media controllati dallo Stato, account social automatizzati e operazioni clandestine di propaganda, la Russia ha cercato di influenzare la percezione del conflitto sia all'interno del proprio paese che a livello internazionale. Uno degli strumenti principali in questo contesto è stata la diffusione di *fake news* e contenuti manipolati con l'obiettivo di screditare il governo ucraino, seminare divisione tra gli alleati occidentali e giustificare l'invasione agli occhi dell'opinione pubblica russa. Piattaforme come Telegram, Twitter e Facebook sono state inondate da narrazioni distorte, promosse da reti di bot e troll gestite da gruppi vicini al Cremlino. Un esempio emblematico di questa strategia è stata la campagna di disinformazione volta a dipingere il governo ucraino come un regime neonazista, un tema ripetutamente enfatizzato dalla propaganda russa per legittimare l'invasione. Allo stesso modo, sono stati orchestrati attacchi informatici mirati alla diffusione di notizie false su presunte atrocità commesse dalle forze ucraine, con l'intento di destabilizzare l'opinione pubblica e alimentare il conflitto interno nel paese. Di fronte alla crescente minaccia del cyberspionaggio come strumento di guerra ibrida, l'Ucraina ha dovuto potenziare significativamente le proprie capacità di difesa cibernetica. Grazie al supporto di attori internazionali, tra cui governi occidentali e aziende specializzate in sicurezza informatica, Kiev è riuscita a mitigare l'impatto di numerosi attacchi e a rafforzare la resilienza delle proprie infrastrutture digitali. Uno degli elementi chiave nella risposta ucraina è stata la creazione dell'*IT Army of Ukraine,* una rete di hacker volontari che ha condotto operazioni di controspionaggio e attacchi informatici contro obiettivi russi. Questa struttura, che ha coinvolto esperti di cybersecurity da tutto il mondo, ha dimostrato come il cyberspazio possa essere utilizzato non solo come arma offensiva, ma anche come strumento di difesa attiva. Parallelamente, le organizzazioni internazionali e le alleanze di cybersicurezza, come il *Cyber Rapid Response Team* dell'Unione Europea e le agenzie di intelligence occidentali, hanno fornito un supporto costante all'Ucraina

nel monitoraggio e nella neutralizzazione delle minacce informatiche. La crescente cooperazione tra pubblico e privato, con il coinvolgimento di aziende come Microsoft e Google, ha permesso di identificare e bloccare in tempi rapidi molte delle campagne di spionaggio e disinformazione condotte dalla Russia. [4445]

## 3.2 Violazioni del diritto internazionale umanitario (spionaggio contro infrastrutture civili, attacchi informatici mirati).

Il conflitto russo-ucraino ha sollevato importanti questioni in materia di diritto internazionale umanitario (DIU), in particolare per quanto riguarda l'uso del cyberspionaggio e degli attacchi informatici diretti contro infrastrutture civili. Il diritto internazionale umanitario, codificato principalmente nelle Convenzioni di Ginevra e nei relativi Protocolli Aggiuntivi, stabilisce norme volte a proteggere la popolazione civile e a limitare gli effetti dei conflitti armati. Tuttavia, l'evoluzione della guerra moderna, caratterizzata da una crescente integrazione di operazioni cibernetiche, ha evidenziato la difficoltà di applicare queste norme ai nuovi scenari bellici. Le operazioni di cyberspionaggio e gli attacchi informatici perpetrati nel corso del conflitto hanno colpito non solo obiettivi militari, ma anche infrastrutture essenziali per la popolazione civile, sollevando interrogativi sulla conformità di tali azioni al quadro normativo internazionale. In particolare, le violazioni del DIU si sono manifestate attraverso attacchi mirati contro il settore energetico, le telecomunicazioni e i servizi sanitari, compromettendo la sicurezza e il benessere dei civili. Il diritto internazionale umanitario stabilisce il principio fondamentale di distinzione, secondo cui le parti in conflitto devono distinguere tra obiettivi militari e beni di carattere civile, risparmiando quest'ultimi da attacchi diretti. Tale principio è codificato nell'Articolo 48 del Protocollo Aggiuntivo I alle Convenzioni di Ginevra, che impone agli Stati l'obbligo di limitare le operazioni militari esclusivamente agli obiettivi legittimi. Nell'ambito del cyberspazio, questa distinzione si è rivelata particolarmente complessa, poiché molte infrastrutture digitali hanno una natura *dual-use*, ovvero servono sia scopi

[44] *V.Poitevin, Il ricorso alla cyber nella cyberguerra russo-ucraina: analisi strategica di un esordio importante, 2024, stormshiel.com,*

[45] *O.Terragni, Cyber spionaggio Russia-Ucraina: tra campagne malware e copycat,2025, redhotcyber.com,* (Ucraina-Condanna degli attacchi russi che hanno colpito delle infrastutture civili , 2024) (A.Calabrese, 2024)

militari che civili. Tuttavia, il diritto internazionale vieta espressamente attacchi indiscriminati o sproporzionati che possano arrecare danni significativi alla popolazione civile. L'Articolo 52 del Protocollo Aggiuntivo I definisce ulteriormente gli obiettivi legittimi, stabilendo che le infrastrutture civili non possono essere oggetto di attacchi a meno che non siano effettivamente utilizzate per scopi militari. Ciò implica che un cyberattacco mirato alla rete elettrica di un Paese, che fornisce energia sia a strutture civili che a basi militari, potrebbe violare il diritto internazionale se causa danni eccessivi ai civili rispetto al vantaggio militare ottenuto. Nel contesto del conflitto russo-ucraino, l'uso di attacchi informatici contro le infrastrutture critiche ha sollevato preoccupazioni per la conformità delle operazioni militari russe al diritto internazionale. Le autorità ucraine e diverse organizzazioni internazionali hanno denunciato ripetuti attacchi cibernetici contro il sistema sanitario, la rete di comunicazioni e le strutture di approvvigionamento energetico, evidenziando una sistematica violazione del DIU. Uno degli episodi più rilevanti in termini di violazioni del diritto internazionale umanitario nel cyberspazio riguarda gli attacchi condotti contro la rete elettrica ucraina. Nel dicembre 2015, il malware *Industroyer* è stato utilizzato per compromettere il sistema di distribuzione dell'energia, causando blackout in diverse regioni del paese. Attacchi simili si sono ripetuti nel corso del conflitto, con ripercussioni significative sulla popolazione civile. Queste operazioni sollevano questioni giuridiche di rilievo: il sabotaggio delle infrastrutture critiche civili è vietato dal DIU, a meno che tali infrastrutture non siano direttamente impiegate per operazioni belliche. Tuttavia, nel caso della rete elettrica, la sua funzione primaria è garantire servizi essenziali alla popolazione, tra cui ospedali, scuole e abitazioni private. L'attacco a queste infrastrutture potrebbe configurarsi come una violazione dell'Articolo 54 del Protocollo Aggiuntivo I, che vieta espressamente l'uso della fame come metodo di guerra e la distruzione di beni indispensabili alla sopravvivenza della popolazione civile. [46] Dal punto di vista giuridico, tali attacchi potrebbero violare l'Articolo 19 della Convenzione di Ginevra IV che tutela le infrastrutture mediche e di emergenza, vietando qualsiasi attacco che possa impedire loro di operare efficacemente. Considerando che molte strutture sanitarie ucraine dipendono dalle telecomunicazioni per il

[46] *Ucraina - Condanna degli attacchi russi che hanno colpito delle infrastrutture civili,2024, it.ambafrance.org,*

coordinamento delle cure e la gestione delle emergenze, il sabotaggio della rete di comunicazione potrebbe costituire una violazione diretta del diritto internazionale umanitario. Oltre agli attacchi diretti alle infrastrutture critiche, il cyberspionaggio ha svolto un ruolo centrale nelle operazioni russe, con ripercussioni significative sulla sicurezza e la stabilità del Paese. L'intercettazione di comunicazioni governative, la violazione di database contenenti informazioni sensibili e l'infiltrazione nei sistemi di sicurezza hanno consentito a Mosca di ottenere un vantaggio strategico significativo. Tuttavia, quando tali operazioni colpiscono dati personali, infrastrutture sanitarie o servizi di emergenza, si pongono dubbi sulla loro legittimità alla luce del diritto internazionale. Secondo l'Articolo 37 del Protocollo Aggiuntivo I, l'uso della perfidia – ovvero atti che inducono il nemico a credere che un determinato soggetto o infrastruttura sia protetto per poi attaccarlo – è vietato nel diritto internazionale umanitario. Se un'operazione di cyberspionaggio induce le forze ucraine a condividere informazioni con un sistema apparentemente sicuro, salvo poi utilizzarle per attacchi mirati, ciò potrebbe costituire una violazione delle norme di condotta dei conflitti armati. Inoltre, secondo il Rapporto di Tallinn – un documento di riferimento non vincolante sulla guerra cibernetica nel diritto internazionale – gli Stati sono responsabili per gli attacchi informatici condotti da gruppi hacker affiliati o sponsorizzati, se vi è una chiara connessione con il governo. Dato il coinvolgimento di gruppi come *APT28 (Fancy Bear),* legati ai servizi segreti russi, il principio della responsabilità statalediventa un elemento chiave per valutare le violazioni del DIU. La tutela dei civili e delle infrastrutture essenziali deve rimanere un principio cardine del diritto internazionale, anche nell'era della guerra digitale. [47]

[47] *A.Calabrese, L'applicazione del diritto umanitario alle operazioni cyber in guerra, 2024, geopolitica.info,*

## 3.3 Analisi delle risposte della comunità internazionale, incluse le sanzioni e i meccanismi di attribuzione degli attacchi.

Il cyberspionaggio e gli attacchi informatici condotti nel contesto del conflitto russo-ucraino hanno sollevato interrogativi giuridici rilevanti per il diritto internazionale, in particolare per quanto riguarda la responsabilità degli Stati e le misure adottate dalla comunità internazionale per contrastare tali operazioni [48] .Le violazioni attribuite alla Federazione Russa, che spaziano dall'infiltrazione nei sistemi governativi e militari ucraini fino agli attacchi informatici diretti contro infrastrutture critiche e servizi essenziali, hanno spinto le organizzazioni internazionali e gli Stati a rispondere attraverso strumenti diplomatici, economici e normativi. La risposta della comunità internazionale si è articolata su due piani principali: da un lato, l'imposizione di sanzioni economiche e restrizioni diplomatiche volte a disincentivare ulteriori operazioni di cyberspionaggio e cyberattacchi; dall'altro, il potenziamento dei meccanismi di attribuzione degli attacchi informatici, un elemento cruciale per garantire l'applicazione del diritto internazionale e il principio di responsabilità statale. L'attribuzione degli attacchi informatici e la conseguente imposizione di misure sanzionatorie trovano fondamento nel diritto internazionale consuetudinario e nei principi sanciti dalla Carta delle Nazioni Unite. In particolare, l'Articolo 2(4) della Carta ONU proibisce l'uso della forza nelle relazioni internazionali, mentre l'Articolo 51 riconosce il diritto all'autodifesa in caso di attacco armato. Sebbene il diritto internazionale non fornisca una definizione univoca della "forza" nel contesto del cyberspazio, gli attacchi informatici di entità significativa – specialmente quelli che compromettono infrastrutture critiche e servizi essenziali – possono essere interpretati come atti ostili suscettibili di ritorsioni. Un elemento chiave nella risposta della comunità internazionale è il principio della responsabilità statale. Secondo l'Articolo 8 degli Articoli sulla Responsabilità degli Stati per Atti Internazionalmente Illegali della Commissione di Diritto Internazionale delle Nazioni Unite (ARSIWA), uno Stato può essere ritenuto responsabile di atti compiuti da attori privati (ad esempio, gruppi hacker) se tali operazioni sono

[48] (UK sanctions cyber-crime gang it says Russia charged with attacking Nato, 2024) *E.Corsi,La Nato a difesa del cyber spazio? Il dilemma nel diritto internazionale, 2018,*

condotte sotto il controllo o con il sostegno dello Stato stesso. Il Tallinn Manual 2.0, pur non essendo un documento vincolante, rappresenta una guida di riferimento per l'applicazione del diritto internazionale ai conflitti cibernetici. Secondo le sue disposizioni, gli attacchi informatici condotti da uno Stato o da attori statali possono configurare una violazione della sovranità territoriale e, nei casi più gravi, un atto di guerra. Tuttavia, il principale ostacolo all'applicazione di misure sanzionatorie e ritorsioni giuridicamente legittime è rappresentato dalla difficoltà di attribuire con certezza gli attacchi informatici a un determinato Stato, rendendo necessario lo sviluppo di meccanismi di attribuzione più efficaci. L'attribuzione di un attacco informatico è un passaggio cruciale per la legittimità delle contromisure adottate dalla comunità internazionale. Senza una chiara identificazione della fonte dell'attacco, qualsiasi ritorsione – sia essa diplomatica, economica o militare – rischia di violare il principio della proporzionalità e dell'obbligo di verificare i fatti prima di adottare misure punitive. Attualmente, i principali strumenti utilizzati per l'attribuzione degli attacchi cibernetici includono: l'Analisi forense digitale: Le agenzie di cybersecurity e le istituzioni governative conducono indagini approfondite sui codici dei malware utilizzati, sulle infrastrutture di comando e controllo e sui pattern operativi degli attaccanti per risalire alla loro origine. Ad esempio, nel caso dell'attacco a Viasat nel 2022, gli esperti hanno identificato collegamenti con gruppi hacker russi, la condivisione di intelligence tra Stati: Organizzazioni internazionali come la NATO e l'Unione Europea hanno rafforzato la cooperazione in materia di cybersecurity, istituendo task force dedicate all'analisi e all'attribuzione delle minacce cibernetiche le Dichiarazioni ufficiali e attribuzioni politiche: Negli ultimi anni, diversi Stati hanno adottato la pratica di rilasciare dichiarazioni ufficiali in cui attribuiscono specifici attacchi a determinati governi. Ad esempio, nel 2022, gli Stati Uniti e il Regno Unito hanno pubblicamente attribuito a gruppi russi l'attacco contro reti governative ucraine. Nonostante questi progressi, il problema dell'attribuzione resta complesso: gli attacchi informatici possono essere condotti attraverso *proxy,* sfruttando infrastrutture in paesi terzi per mascherare la loro origine, e molti Stati negano ufficialmente il coinvolgimento nelle operazioni cibernetiche. In risposta agli attacchi informatici e alle operazioni di cyberspionaggio condotte dalla Russia, la comunità internazionale ha adottato una serie di sanzioni economiche e restrizioni diplomatiche. L'Unione Europea,

gli Stati Uniti, il Regno Unito e altri attori hanno implementato misure mirate per limitare la capacità della Russia di condurre operazioni cibernetiche offensive.

Le principali sanzioni adottate includono:[49]

- Sanzioni contro individui e gruppi responsabili di attacchi informatici: L'UE e gli USA hanno inserito nella loro lista nera hacker e funzionari russi legati a operazioni di cyberspionaggio, congelandone i beni e vietandone l'ingresso nei loro territori.
- Restrizioni tecnologiche: Sono stati imposti divieti sull'esportazione di tecnologie avanzate, inclusi software e hardware utilizzabili per operazioni di intelligence e guerra informatica.
- Esclusione della Russia da organismi internazionali di cooperazione in cybersicurezza: La Russia è stata esclusa da diverse iniziative di collaborazione in ambito cibernetico, limitandone la possibilità di accedere a informazioni strategiche condivise a livello internazionale.

L'efficacia di tali misure resta un tema dibattuto. Sebbene abbiano contribuito a limitare le capacità operative di alcuni gruppi hacker russi, non hanno impedito alla Federazione Russa di continuare a condurre operazioni di cyberspionaggio e attacchi informatici, dimostrando la necessità di ulteriori strumenti giuridici per contrastare le minacce cibernetiche a livello internazionale. L'analisi del cyberspionaggio alla luce del diritto internazionale ha evidenziato come questo fenomeno rappresenti una delle principali sfide della sicurezza globale contemporanea. I casi Wikileaks, Datagatee il conflitto russo-ucraino dimostrano come le operazioni di intelligence e spionaggio informatico abbiano ormai assunto una dimensione transnazionale, sollevando questioni giuridiche complesse legate alla tutela della sovranità statale, alla protezione della privacy e alla sicurezza delle infrastrutture critiche. Il caso Wikileaks, con la diffusione di documenti riservati provenienti da governi e organizzazioni internazionali, ha sollevato interrogativi sul bilanciamento tra il diritto all'informazione e la necessità di proteggere dati sensibili per la sicurezza nazionale. Da un lato, la trasparenza e il diritto di cronaca sono principi cardine nelle democrazie moderne,

[49] *UK sanctions cyber-crime gang it says Russia charged with attacking NATO, 2024, reuters.com,*

ma dall'altro, la divulgazione di informazioni classificate ha esposto governi e cittadini a potenziali minacce, rivelando il delicato confine tra informazione e spionaggio. Il Datagate, con il coinvolgimento della National Security Agency (NSA) degli Stati Uniti, ha messo in luce l'estensione delle attività di sorveglianza su scala globale. Le rivelazioni di Edward Snowden hanno dimostrato come le tecnologie di cyberspionaggio possano essere utilizzate non solo per il contrasto al terrorismo e alla criminalità, ma anche per attività di controllo su cittadini, aziende e istituzioni internazionali, sollevando dubbi sulla conformità di tali operazioni con il diritto internazionale. Il principio di non ingerenza negli affari interni di uno Stato, sancito dal diritto internazionale consuetudinario e dalla Carta delle Nazioni Unite, è stato violato in diverse occasioni, alimentando il dibattito sulla necessità di un quadro normativo più chiaro per regolamentare le operazioni di sorveglianza digitale. Nel conflitto russo-ucraino, il cyberspionaggio si è trasformato in un vero e proprio strumento di guerra ibrida, con attacchi mirati alle infrastrutture critiche, operazioni di disinformazione e tentativi di destabilizzazione politica. La comunità internazionale ha risposto con l'adozione di sanzioni e meccanismi di attribuzione degli attacchi, ma le difficoltà nel dimostrare il coinvolgimento diretto degli Stati e l'assenza di un quadro giuridico vincolante nel diritto internazionale hanno reso complesso l'applicazione di misure efficaci. La protezione delle infrastrutture civili dagli attacchi informatici rimane un punto critico, poiché la guerra cibernetica si sviluppa in un contesto in cui le *orme del diritto internazionale umanitario*sono spesso difficili da applicare in modo chiaro ed efficace. Le problematiche emerse nei casi analizzati rendono evidente la necessità di nuovi strumenti per il contrasto al cyberspionaggio e alla guerra informatica. In questo contesto, l'intelligenza artificiale sta emergendo come una possibile risorsa in grado di migliorare le capacità di difesa e prevenzione degli attacchi informatici. L'IA, attraverso l'analisi avanzata dei dati, il riconoscimento delle minacce in tempo reale e lo sviluppo di sistemi di protezione autonomi, può rappresentare un elemento chiave per il rafforzamento della sicurezza cibernetica a livello internazionale.

# Conclusione

Il prossimo capitolo approfondirà il potenziale dell'intelligenza artificiale nel contrasto al cyberspionaggio, esplorando le sue applicazioni nelle operazioni di intelligence, nella sicurezza delle infrastrutture digitali e nel rafforzamento delle strategie di difesa informatica. Inoltre, verranno analizzate le possibili implicazioni etiche e giuridiche legate all'uso dell'IA nel cyberspazio, con particolare attenzione alla necessità di regolamentazioni che ne garantiscano un impiego conforme ai principi del diritto internazionale. L'adozione di nuove tecnologie nella lotta al cyberspionaggio rappresenta una sfida cruciale per il futuro della sicurezza globale, e l'IA potrebbe costituire uno strumento determinante per la protezione dei dati sensibili e la prevenzione delle minacce informatiche, contribuendo così a un cyberspazio più sicuro e regolamentato.

# CAPITOLO III

# Il futuro dello spionaggio informatico

Nel terzo capitolo della presente tesi si esamina in profondità il duplice impatto dell'Intelligenza Artificiale (IA) sullo spionaggio informatico, mettendo in luce sia le potenzialità che i rischi associati a questa tecnologia. L'IA, grazie alla sua capacità di processare enormi volumi di dati e di identificare pattern complessi, si configura come uno strumento decisivo per il rilevamento e la prevenzione di operazioni di spionaggio. Gli algoritmi di apprendimento automatico consentono di individuare anomalie e comportamenti atipici nelle reti, rilevando tempestivamente tentativi di accesso non autorizzati e nuove modalità di intrusione che sfuggirebbero ai sistemi di sicurezza tradizionali basati su regole predefinite. Questa tecnologia, infatti, offre una protezione proattiva, permettendo di identificare e neutralizzare le minacce prima che possano compromettere la sicurezza dei dati sensibili. Tuttavia, l'impiego dell'IA nel contesto dello spionaggio informatico presenta anche criticità significative. Oltre al rischio che gli stessi algoritmi possano essere manipolati attraverso tecniche di machine learning contraddittorio, esiste la possibilità che la tecnologia, se non gestita correttamente, diventi uno strumento nelle mani di attori malintenzionati. La gestione dei dati, spesso estremamente sensibili, e la carenza di esperti specializzati nel settore costituiscono ulteriori sfide, richiedendo un approccio che sappia bilanciare innovazione e sicurezza. In questo capitolo si discuterà inoltre dell'importanza di potenziare i sistemi di autenticazione mediante tecnologie biometriche e analisi comportamentale, oltre che dell'integrazione di piattaforme che automatizzano e coordinano le operazioni di difesa. Verranno analizzate le strategie volte a sfruttare le potenzialità dell'IA per rafforzare le contromisure contro le operazioni di spionaggio, evidenziando come la collaborazione tra enti pubblici, privati e istituzioni accademiche rappresenti un elemento chiave per sviluppare soluzioni efficaci e resilienti. Attraverso l'analisi di casi concreti e l'esame delle tecnologie emergenti, il capitolo si propone di fornire una visione completa sulle sfide e le opportunità che l'IA offre nella lotta contro lo spionaggio informatico, sottolineando la necessità di un approccio multilivello che combini

l'innovazione tecnologica con il know-how umano per garantire un ambiente digitale sicuro e protetto.[50]

## 1 L'evoluzione delle difese cyber

L'evoluzione delle difese cyber rappresenta un percorso dinamico e complesso, in cui si intrecciano aspetti tecnologici, strategici e normativi, con un impatto rilevante anche sul diritto internazionale. Inizialmente, le prime misure di sicurezza digitale si fondavano su strumenti statici, quali firewall e antivirus, progettati per bloccare attacchi noti e prevenire l'accesso non autorizzato attraverso regole fisse. Queste soluzioni, sebbene efficaci in un contesto caratterizzato da minacce relativamente semplici e ben catalogate, hanno evidenziato presto i limiti quando si è assistito a una crescente sofisticazione degli attacchi, inclusi quelli finalizzati allo spionaggio informatico. Con l'espansione del panorama digitale, le tecniche di difesa si sono progressivamente evolute adottando sistemi di rilevamento delle intrusioni (IDS) e monitoraggi in tempo reale, capaci di identificare anomalie e comportamenti sospetti. Tuttavia, la complessità degli attacchi moderni ha richiesto un approccio che andasse ben oltre la semplice analisi basata su firme predefinite. È in questo contesto che le tecnologie avanzate, come il Machine Learning e l'Intelligenza Artificiale, hanno rivoluzionato le strategie di protezione, permettendo di analizzare grandi volumi di dati e di riconoscere pattern complessi, anche in scenari altamente dinamici e imprevedibili. Questi sistemi intelligenti, in grado apprendere e adattarsi in modo continuo, hanno reso possibile una difesa più proattiva, capace di anticipare le minacce e intervenire tempestivamente per ridurre i danni in caso di operazioni di spionaggio informatico. Parallelamente all'innovazione tecnologica, si è assistito a una trasformazione del paradigma di sicurezza, che ha abbracciato un approccio multilivello e integrato. Tale modello non si limita più a reagire agli incidenti, ma punta a una prevenzione strutturata che combina l'adozione di tecnologie d'avanguardia, la formazione continua del personale e la collaborazione intersettoriale. La crescente complessità delle minacce ha spinto inoltre alla condivisione di informazioni e buone pratiche tra enti pubblici, privati e istituzioni accademiche, creando reti di cooperazione che trascendono i confini nazionali. Quest'ultima dinamica ha assunto particolare rilievo anche nell'ambito del diritto

[50] *F.Livelli, Così l'intelligenza artificiale sta rivoluzionando la cyber security, 2023,*

internazionale, il quale si trova oggi ad affrontare sfide nuove e inedite poste dalla cybersfera. L'interconnessione globale delle infrastrutture digitali e la natura transnazionale degli attacchi informatici richiedono un coordinamento giuridico a livello internazionale per stabilire norme condivise e meccanismi di cooperazione. (F.Livelli, 2023) (J.D.Ohlin, 2015) (Il ruolo dell'intelligenza artificiale per la sicurezza informatica, 2024) (Europea) (F.Niola, 2024) (M.Santarelli, 2022) (group) (C.Gallotti, 2024)

## 1.1 Strategie di inganno

Volendo esaminare in maniera integrata l'evoluzione delle difese cibernetiche e delle operazioni di inganno nel contesto dei conflitti moderni si può evidenziare come tali dinamiche si intreccino con il fenomeno dello spionaggio informatico. In un'epoca in cui, contrariamente al secolo scorso in cui il movimento e la manovra costituivano i cardini dell'arte militare, il dominio del cyberspazio e la manipolazione dell'informazione assumono un ruolo strategico centrale, la capacità di proteggere le infrastrutture digitali e, al contempo, di operare inganni sul nemico, diventa determinante per ottenere e mantenere un vantaggio competitivo. L'analisi delle recenti esperienze operative nel cyberspazio evidenzia come le attività di inganno possano condurre, in determinati casi, a far assumere all'attore cibernetico il ruolo di "attaccante" legale, con conseguenti responsabilità derivanti dall'obbligo di adottare tutte le precauzioni necessarie per evitare danni collaterali, come previsto dall'Articolo 57 del Protocollo Aggiuntivo I alle Convenzioni di Ginevra. Allo stesso tempo, operazioni che alterano l'affidabilità delle informazioni su cui si basano le decisioni di targeting – ad esempio, mediante la sostituzione di dati reali con informazioni false – rischiano di compromettere il rispetto dei principi di distinzione, proporzionalità e precauzione, esponendo la parte vittima di tali manovre a conseguenze gravi e, talvolta, a danni a civili o oggetti protetti. In questo contesto, il fenomeno dello spionaggio informatico si configura come una delle espressioni più insidiose di queste dinamiche: se da un lato il cyber inganno può essere utilizzato per mascherare le operazioni di raccolta di informazioni, dall'altro esso pone la questione dell'attribuibilità e della responsabilità, aggravando ulteriormente il dilemma giuridico. Le operazioni di spionaggio informatico, caratterizzate da un accesso non autorizzato e dalla manipolazione segreta dei dati, si avvalgono

spesso di tecniche ingannevoli che ne complicano l'analisi dal punto di vista del diritto internazionale, che tradizionalmente ha fatto affidamento su concetti come la "trasparenza" e l'attribuibilità delle azioni per regolare l'uso della forza. Pertanto, l'evoluzione delle difese cibernetiche e delle strategie di inganno, unite alla crescente importanza del cyber spionaggio, richiedono un ripensamento sia degli strumenti tecnologici che dei meccanismi normativi. È necessario, infatti, sviluppare sistemi in grado di rilevare e contrastare le interferenze e le manipolazioni dei dati, garantendo al contempo che le azioni intraprese rispettino i principi fondamentali del diritto internazionale umanitario. In questo modo, la protezione delle infrastrutture critiche e la sicurezza delle operazioni militari potranno essere assicurate anche in un ambiente in cui l'informazione è al centro del conflitto. L'integrazione tra inganno cibernetico e spionaggio informatico rappresenta un aspetto cruciale della moderna guerra digitale, in cui il cyberspazio diventa il nuovo campo di battaglia. Le sfide poste dalla manipolazione dell'informazione e dalla difficoltà di attribuire in modo preciso le operazioni rendono imprescindibile lo sviluppo di nuove strategie difensive e di un quadro normativo aggiornato, capace di governare in modo efficace le attività ostili e di proteggere i principi di distinzione e proporzionalità, fondamentali per il rispetto del diritto internazionale. [51]

[51] *J.D.Ohlin, Cyber War: Law and Ethics for Virtual Conflicts, 2015,*

# 2 Il ruolo dell'intelligenza artificiale nel cyberspionaggio

I metodi tradizionali di sicurezza informatica, basati sull'applicazione di regole e pattern predefiniti, stanno dimostrando progressivamente la loro insufficienza di fronte alle minacce dinamiche e in continua evoluzione che caratterizzano il panorama digitale odierno. In risposta a questo scenario, sorge la necessità di adottare soluzioni di sicurezza più sofisticate e adattabili, in grado di fronteggiare attacchi sempre più complessi e mirati a un'ampia gamma di asset, dai dati personali e finanziari alle infrastrutture critiche e alla sicurezza nazionale. In questo contesto, l'Intelligenza Artificiale (IA) emerge come attore cruciale, grazie alla capacità degli algoritmi di machine learning e deep learning di elaborare enormi quantità di dati, riconoscere schemi e identificare anomalie in tempo reale. Le soluzioni di sicurezza informatica basate sull'IA, infatti, offrono una difesa dinamica e contestualmente consapevole, in grado di adattarsi alle minacce emergenti e di mitigare proattivamente i rischi. Tali sistemi, sfruttano l'apprendimento continuo, permettono alle organizzazioni di anticipare gli attacchi e di rispondere tempestivamente, contribuendo a rafforzare la resilienza complessiva degli asset digitali. Tuttavia, l'adozione dell'IA nel campo della sicurezza informatica non è priva di sfide e problematiche etiche. La necessità di accedere a grandi volumi di dati per addestrare i modelli comporta significative preoccupazioni in tema di privacy e protezione dei dati, soprattutto alla luce delle normative vigenti quali il GDPR e il CCPA. Inoltre, i sistemi basati sull'IA risultano vulnerabili agli attacchi avversari, nei quali hacker possono manipolare gli input per compromettere l'affidabilità delle difese. Queste problematiche richiedono lo sviluppo di robuste contromisure e di una governance attenta, capace di salvaguardare l'integrità dei sistemi e di garantire il rispetto dei principi etici. Un ulteriore aspetto critico riguarda la necessità di una collaborazione sinergica tra uomo e macchina. Piuttosto che considerare l'IA come un semplice sostituto degli analisti umani, è fondamentale promuovere il concetto di intelligenza aumentata, in cui le capacità decisionali degli operatori vengano potenziate dalla tecnologia. Ciò implica, da- un lato, investimenti significativi nello sviluppo di competenze specifiche e, dall'altro, la creazione di una cultura collaborativa che favorisca l'interazione efficace tra sistemi intelligenti e professionisti della sicurezza informatica. Nel quadro della mia tesi sullo spionaggio informatico, questa analisi delle evoluzioni delle difese digitali e delle

strategie basate sull'IA si inserisce in un contesto più ampio, evidenziando come la manipolazione e l'inganno informatico rappresentino strumenti sempre più utilizzati sia per la protezione che per l'attacco. Le tecnologie di IA, infatti, non solo rafforzano le difese contro minacce sempre più sofisticate, ma possono anche essere impiegate per condurre operazioni di spionaggio informatico, in cui la raccolta e la manipolazione dei dati assumono un ruolo centrale. In questo senso, l'evoluzione delle difese cyber si intreccia strettamente con il fenomeno dello spionaggio informatico, rendendo necessaria una riflessione approfondita sia sui benefici che sui rischi associati all'adozione dell'IA in ambito di sicurezza. L'IA offre un potenziale trasformativo per le strategie di sicurezza informatica, migliorando la capacità di rilevazione e prevenzione delle minacce e contribuendo a una gestione più efficace degli asset digitali. Tuttavia, per sfruttare appieno tali opportunità, è indispensabile affrontare con serietà le sfide etiche, di privacy e di sicurezza legate all'adozione di tecnologie avanzate, promuovendo una visione integrata che unisca innovazione tecnologica e rigore normativo. Solo così sarà possibile garantire la protezione delle infrastrutture digitali e contrastare efficacemente il fenomeno dello spionaggio informatico.[52]

[52] *Il ruolo dell'intelligenza artificiale per la sicurezza informatica, 2024, cyberdivision.net,*

## 2.1 Normativa europea sull'intelligenza artificiale

La normativa sull'Intelligenza Artificiale rappresenta il primo vero e proprio quadro giuridico globale in materia, volto ad affrontare i rischi connessi all'uso di tali tecnologie e a posizionare l'Europa come leader mondiale in questo ambito. Il Regolamento (UE) 2024/1689, che introduce norme armonizzate sull'IA, mira a garantire lo sviluppo di un'IA affidabile e sicura, integrandosi in un più ampio pacchetto di misure che promuovono innovazione, investimenti e un approccio antropocentrico alle nuove tecnologie[53]. Questa legge adotta un approccio basato sul rischio, distinguendo quattro livelli di rischio per i sistemi di IA: rischio inaccettabile, ad alto rischio, rischio di trasparenza e rischio minimo o nullo. I sistemi considerati a rischio inaccettabile, ossia quelli che rappresentano una chiara minaccia per la sicurezza, il benessere e i diritti delle persone, sono vietati. Tra questi rientrano pratiche come l'inganno e la manipolazione dannosi, l'utilizzo sfruttatore delle vulnerabilità, il punteggio sociale, la valutazione del rischio di reato individuale, la raccolta indiscriminata di dati per il riconoscimento facciale, il riconoscimento delle emozioni in ambienti sensibili, la categorizzazione biometrica per dedurre caratteristiche protette e l'identificazione biometrica remota in tempo reale in spazi pubblici. I sistemi di IA ad alto rischio, che possono avere un impatto significativo sulla salute, sulla sicurezza o sui diritti fondamentali, sono soggetti a obblighi stringenti prima della loro immissione sul mercato. Questi obblighi includono, ad esempio, la predisposizione di sistemi di valutazione e mitigazione dei rischi, l'utilizzo di dataset di alta qualità per ridurre al minimo i risultati discriminatori, la registrazione e tracciabilità delle attività, una documentazione dettagliata e chiara per gli operatori, nonché l'adozione di misure di sorveglianza umana e di elevati standard di robustezza e cibersicurezza. Un'attenzione particolare è riservata al rischio di trasparenza: la normativa impone obblighi di informazione affinché gli utenti siano consapevoli dell'utilizzo di sistemi di IA, per esempio quando interagiscono con chatbot o si trovano ad affrontare contenuti generati automaticamente, come deep fake. In questo modo, si intende preservare la fiducia degli utenti e consentire decisioni informate. La maggior parte delle applicazioni di IA, però, rientra nella categoria a rischio minimo o nullo, per le quali non sono previste norme specifiche, come

[53] *Legge sull'intelligenza artificiale, Commissione Europea,*

nel caso di videogiochi o filtri antispam. Per i fornitori di sistemi di IA ad alto rischio, il nuovo regolamento prevede una procedura dettagliata per la dichiarazione di conformità, che va dalla fase pre-commercializzazione con valutazioni e monitoraggi continui – fino alla sorveglianza post-commercializzazione, durante la quale vengono segnalati eventuali incidenti o malfunzionamenti. Un'ulteriore attenzione è dedicata ai modelli di IA per uso generale, che sebbene versatili, potrebbero comportare rischi sistemici qualora fossero ampiamente adottati. Per questi modelli sono previste specifiche norme di trasparenza e misure di mitigazione dei rischi, norme che entreranno in vigore a partire da agosto 2025, supportate dallo sviluppo di un codice di buone pratiche da parte dell'Ufficio per l'IA. La governance di questo nuovo quadro normativo è strutturata e partecipativa: l'Ufficio europeo per l'IA, istituito nel febbraio 2024, sovrintende all'attuazione delle norme insieme a organi consultivi quali il Comitato europeo per l'Intelligenza Artificiale, un gruppo di esperti scientifici indipendenti e un foro consultivo che coinvolge rappresentanti di diversi settori. Tale struttura garantisce un approccio equilibrato e condiviso nell'applicazione della legge, che diventerà progressivamente operativa, con alcune disposizioni in vigore già dal 2 febbraio 2025 e la piena applicazione prevista per il 2 agosto 2026 (con un periodo di transizione fino al 2 agosto 2027 per i sistemi ad alto rischio integrati in prodotti regolamentati). Questa regolamentazione non solo intende rafforzare la fiducia degli utenti nelle tecnologie emergenti, ma anche prevenire gli effetti indesiderati che potrebbero derivare da decisioni automatizzate, in contesti sensibili come il reclutamento, l'erogazione di servizi pubblici e la gestione della giustizia. Nel contesto della mia tesi sullo spionaggio informatico, questo nuovo quadro normativo assume particolare rilevanza. Infatti, la disciplina rigorosa e trasparente dei sistemi di IA contribuisce non solo a migliorare la sicurezza informatica e la protezione degli asset digitali, ma incide anche sulle modalità con cui tali tecnologie possono essere sfruttate per attività di spionaggio e manipolazione delle informazioni. Mentre l'IA offre notevoli opportunità in termini di rilevamento e prevenzione delle minacce, essa comporta anche il rischio di essere utilizzata per operazioni di spionaggio informatico, mettendo a repentaglio la trasparenza e l'affidabilità dei dati. In questo senso, il quadro normativo europeo si configura come uno strumento fondamentale non solo per garantire la sicurezza, ma anche per proteggere i diritti fondamentali,

contribuendo a creare un ecosistema in cui innovazione e rispetto delle norme etiche e giuridiche coesistono. La legge sull'IA rappresenta una pietra miliare per la regolamentazione delle tecnologie emergenti, fornendo un modello che coniuga innovazione e tutela dei diritti. L'approccio basato sul rischio, insieme a un sistema di governance articolato e a stringenti obblighi per i fornitori di sistemi ad alto rischio, mira a garantire lo sviluppo di un'IA sicura e affidabile. Questo quadro normativo si inserisce perfettamente nel contesto della sicurezza informatica e dello spionaggio informatico, tematiche centrali della mia tesi, e costituisce uno strumento essenziale per promuovere un utilizzo responsabile e trasparente delle nuove tecnologie.

## 2.2 La Convenzione sull'IA del Consiglio d'Europa: Il Primo Quadro Normativo Internazionale per la Tutela dei Diritti Umani"[54]

Nel contesto dell'attuale mancanza di una normativa internazionale organica e vincolante sull'intelligenza artificiale, la Convenzione del Consiglio d'Europa sull'Intelligenza Artificiale (CETS 225) rappresenta un primo e significativo tentativo di colmare questa lacuna. Questo trattato, firmato non solo da numerosi Paesi europei, ma anche da Stati non appartenenti all'UE – tra cui gli Stati Uniti, Israele, Regno Unito, questa convenzione costituisce il primo testo normativo globalmente vincolante finalizzato a tutelare i diritti umani nell'ambito dell'IA. La Convenzione si propone di trovare un equilibrio tra il rapido sviluppo tecnologico e la necessità di proteggere i principi fondamentali della democrazia, dello Stato di diritto e dei diritti umani. Essa impone agli Stati firmatari l'obbligo di regolare l'intero ciclo di vita dei sistemi di intelligenza artificiale, ponendo particolare enfasi su trasparenza, accountability e protezione della privacy. In sostanza, il trattato stabilisce una serie di principi e standard minimi che gli Stati devono rispettare per prevenire l'uso distorto dell'IA, soprattutto nei casi in cui queste tecnologie possano compromettere la dignità umana o contribuire a forme di discriminazione. Il testo, adottando un approccio basato sul rischio, prevede misure preventive e valutazioni continue dei potenziali impatti negativi derivanti dall'uso dell'IA. In particolare, esso sollecita gli Stati a vietare l'impiego di tecnologie ritenute incompatibili con i diritti fondamentali, a garantire la trasparenza nei processi decisionali automatizzati e a fornire rimedi efficaci in

[54] *F.Niola, IA il primo trattato internazionale: la Convenzione del Consiglio d'Europa, agendadigitale.eu, 2024,*

caso di violazioni. Tra i principi cardine vi sono il rispetto della dignità umana, il diritto all'uguaglianza e la protezione dei dati personali, che costituiscono le fondamenta su cui si basa l'intero trattato. Un elemento di rilievo è rappresentato dall'articolato del trattato, che, nei suoi primi articoli, definisce gli obiettivi della normativa e impone agli Stati l'adozione di misure legislative e amministrative atte a garantire che l'utilizzo dell'IA non comprometta i diritti fondamentali né l'autonomia delle istituzioni democratiche. In particolare, l'articolo 8 stabilisce il principio di trasparenza e sorveglianza, richiedendo che le decisioni automatizzate siano comprensibili e soggette a controllo, mentre l'articolo 10 sancisce il divieto di discriminazione, imponendo agli Stati di adottare misure idonee a contrastare l'eventuale amplificazione delle disuguaglianze tramite l'uso degli algoritmi. Parallelamente, il trattato prevede la creazione di meccanismi di governance e supervisione, espressi nell'obbligo, previsto dall'articolo 26, di istituire organi indipendenti in grado di monitorare l'applicazione delle disposizioni convenzionali. Inoltre, l'articolo 23 introduce la Conferenza delle Parti, un organismo che facilita la cooperazione internazionale e lo scambio di informazioni tra gli Stati membri, promuovendo una visione globale e coordinata delle problematiche legate all'intelligenza artificiale. Questo primo quadro normativo, che si distingue per la sua portata innovativa, rappresenta un punto di svolta nel diritto internazionale in materia di IA. Esso non solo stabilisce obblighi concreti per la tutela dei diritti umani e la salvaguardia della democrazia, ma contribuisce anche a creare un modello di cooperazione internazionale che va oltre i tradizionali confini sovrani, invitando anche gli Stati non europei a conformarsi a standard comuni. Nel contesto dello spionaggio informatico, l'adozione di questa Convenzione assume una particolare rilevanza. In assenza di una normativa internazionale consolidata, il CETS 225 emerge come il primo tentativo di definire standard minimi globali per un uso responsabile dell'IA, prevenendo abusi e mitigando i rischi che potrebbero compromettere non solo la sicurezza informatica, ma anche la trasparenza e l'accountability nei processi decisionali automatizzati. Questa iniziativa normativa costituisce un modello pionieristico, il cui impatto potrà essere valutato anche in relazione alle dinamiche dello spionaggio informatico, evidenziando come il controllo e la regolamentazione dell'IA siano strumenti indispensabili per proteggere i diritti fondamentali in un mondo sempre più interconnesso e digitalizzato. La

Convenzione del Consiglio d'Europa sull'Intelligenza Artificiale si configura come un primo passo fondamentale verso la creazione di una normativa internazionale efficace sull'IA, ponendo le basi per un uso sicuro, trasparente e rispettoso dei diritti umani. Questo trattato, pur rappresentando ancora un inizio, offre un modello che potrebbe evolversi e influenzare significativamente il futuro del diritto internazionale in un'epoca in cui le tecnologie emergenti, compreso lo spionaggio informatico, giocano un ruolo sempre più centrale.

## 3 Scenari futuri dello spionaggio informatico

Nel contesto di un panorama globale in rapida trasformazione, la recente nomina di Gil Herrera a Direttore della Ricerca della NSA rappresenta un punto di svolta significativo per le attività di intelligence e, in particolare, per gli scenari futuri dello spionaggio informatico. Herrera si trova ora a guidare una delle agenzie di spionaggio più influenti al mondo, con un duplice mandato: proteggere le infrastrutture digitali degli Stati Uniti e condurre operazioni di intelligence a livello globale.[55] Le sfide che si prospettano per la NSA si configurano come il naturale esito dei mutamenti geopolitici e delle innovazioni tecnologiche. Oggi non esiste più una "superpotenza solitaria" impegnata in una guerra fredda tradizionale, bensì un nuovo ordine mondiale in cui Stati Uniti, Cina e Russia si contendono il primato tecnologico e strategico. In questo scenario, la NSA deve fronteggiare non solo la concorrenza di attori statali che sviluppano tecnologie autonome e indipendenti, ma anche di gruppi non statali e attori privati che sfruttano strumenti innovativi per operazioni di spionaggio. A tal proposito, Herrera ha dichiarato la necessità di concentrarsi sugli avversari che non si affidano ai consueti servizi commerciali, ma che costruiscono le proprie tecnologie e infrastrutture. Ciò richiede, a livello di ricerca, lo sviluppo di strumenti capaci di analizzare e interrogare enormi moli di dati, nonché di monitorare in tempo reale i sistemi emergenti, risultato della competizione tra le grandi potenze. In particolare, l'integrazione del calcolo quantistico rappresenta una delle sfide più rilevanti: questa tecnologia, grazie all'algoritmo di Shor, ha il potenziale di rompere le attuali soluzioni crittografiche, mettendo a rischio la protezione dei dati sensibili. L'investimento in progetti quantistici, sostenuto anche dalla NSA e supportato da attori come Google e IBM, evidenzia

[55] *M.Santarelli, NSA lo spionaggio del futuro e i nuovi equilibri geopolitici: le sfide, 2022, agendadigitale.eu*

l'importanza di anticipare e neutralizzare tali minacce. Parallelamente, l'evoluzione tecnologica ha determinato una trasformazione interna nell'organizzazione stessa della NSA. Dalla storica Camera Nera, che operò tra il 1919 e il 1929 per decifrare messaggi telegrafici, fino alla formazione del *Signals Intelligence Service* e all'attuale struttura organizzativa che conta cinque dipartimenti – matematica, fisica, informatica, scienze computazionali e ingegneria elettrica – l'agenzia ha sempre dovuto reinventarsi per restare al passo con le nuove sfide. Oggi, sotto la guida di Herrera, la NSA continua a porsi come un centro di eccellenza nel campo della cybersecurity, sviluppando strumenti come Ghidra per il *reverse engineering* e investendo nella ricerca di nuove architetture computazionali e di soluzioni per la gestione dei Big Data. Inoltre, l'evoluzione delle reti di telecomunicazione, favorita dalla diffusione globale del 5G, sta rimodellando il modo in cui vengono raccolte e analizzate le informazioni. La maggiore velocità, la riduzione dei tempi di latenza e l'ampliamento della connettività offrono nuove opportunità per la raccolta di intelligence, ma allo stesso tempo sollevano sfide notevoli in termini di sicurezza e attribuibilità degli attacchi. In questo scenario, la capacità di integrare le tecnologie di sicurezza informatica con la fisica quantistica e i teoremi matematici diventa fondamentale per costruire un vantaggio strategico e per modellare il futuro dello spionaggio informatico. Le parole di Herrera sottolineano l'importanza di anticipare le trasformazioni tecnologiche: ogni evoluzione comporta inevitabilmente una riformulazione delle sfide da affrontare. La ricerca sul calcolo quantistico, ad esempio, non solo apre nuove frontiere nella crittoanalisi, ma richiede anche un aggiornamento delle tecniche di difesa per proteggere le infrastrutture digitali. Analogamente, il potenziamento delle capacità di raccolta e analisi dei dati, resa possibile dall'adozione di algoritmi di machine learning e sistemi autonomi, trasforma il modo in cui le operazioni di spionaggio vengono concepite e realizzate. In questo contesto, il futuro dello spionaggio informatico si prospetta come una convergenza di discipline: dalla fisica quantistica alla cybersecurity, passando per l'ingegneria elettrica e la matematica, tutti i settori si intrecceranno per fornire le basi di una nuova era dell'intelligence. Queste dinamiche, che spaziano dalla protezione dei sistemi nazionali alle operazioni di spionaggio globale, richiedono una visione integrata e multidimensionale, in cui l'innovazione tecnologica si coniuga con la necessità di rimanere sempre un passo

avanti rispetto agli avversari. Nel complesso, il mandato affidato a Gil Herrera non solo rappresenta un aggiornamento operativo per la NSA, ma incarna anche un invito a ripensare gli scenari futuri dello spionaggio informatico. In un mondo in cui la competizione tecnologica e le trasformazioni geopolitiche si intrecciano in maniera sempre più complessa, la sfida per le agenzie di intelligence sarà quella di anticipare le tendenze emergenti, sfruttare le nuove tecnologie per ottenere un vantaggio strategico e, al contempo, garantire la protezione delle infrastrutture critiche e dei dati sensibili. [56]Ulteriore caso emblematico che si è contraddistinto negli ultimi anni è quello riguardante Tik Tok il social network cinese. Il Congresso degli Stati Uniti e i responsabili delle politiche a livello federale e statale hanno evidenziato come la Repubblica Popolare Cinese rappresenti una seria minaccia per la sicurezza nazionale. Questo pericolo scaturisce dall'approccio strategico della Cina, che mira a coordinare strettamente le aziende private agli interessi statali, influenzando in maniera significativa le piattaforme digitali che operano negli Stati Uniti. Tali piattaforme, infatti, raccolgono enormi quantità di dati e informazioni sensibili, creando così un'opportunità per l'intelligence cinese di sfruttare questi dati a fini geopolitici e di cyberspionaggio. Un esempio emblematico di questa dinamica è rappresentato da TikTok, la popolare piattaforma di social media gestita da ByteDance. A dicembre 2024, TikTok ha dichiarato, in documenti depositati in tribunale, di contare 170 milioni di utenti negli Stati Uniti. Inoltre, il CEO di TikTok ha testimoniato al Congresso nel marzo 2023 che ByteDance conserva i dati degli utenti statunitensi per almeno sette anni, alimentando il timore che tali informazioni possano essere impiegate dal governo cinese per attività di *counterintelligence.* Secondo la valutazione annuale delle minacce del 2024 dell'Office of the Director of National Intelligence (ODNI), la Cina resta l'attore informatico più attivo e persistente, con la capacità di condurre operazioni aggressive non solo contro le reti governative e militari, ma anche contro il settore privato e le infrastrutture critiche. In un'eventualità di conflitto, tali operazioni potrebbero interferire con il processo decisionale statunitense, generando instabilità e panico, e ostacolando il dispiegamento delle forze militari. La strategia cinese di cyberspionaggio non si limita alla raccolta di informazioni: essa è parte integrante di una più ampia

[56] *Meridian group, Il caso Tik Tok, meridian-group.eu,*

proiezione di potenza, un vero e proprio *"cyber soft power"* che mira a influenzare le decisioni politiche ed economiche a livello globale. La Cina, infatti, investe nella penetrazione dei settori critici dei paesi concorrenti per minarne la stabilità e acquisire vantaggi competitivi nei settori della difesa e della sicurezza energetica. Questo modello si basa su una stretta collaborazione tra settore pubblico e privato, in un contesto normativo che impone alle aziende digitali cinesi di cooperare attivamente con il governo, creando così un ecosistema altamente integrato e coordinato per la raccolta e l'utilizzo dei dati. Un recente esempio che illustra la sofisticazione di queste operazioni è rappresentato dal caso *Salt Typhoon*, un attacco informatico contro il Dipartimento del Tesoro degli Stati Uniti. Gli aggressori, presumibilmente sponsorizzati dalla Cina, hanno sfruttato una vulnerabilità in un software di gestione degli accessi privilegiati per accedere a informazioni sensibili, in particolare all'interno dell'Ufficio per il Controllo degli Asset Stranieri (OFAC). Questo attacco, che potrebbe essere interpretato come parte di una strategia di "guerra economica", dimostra come la raccolta e l'esfiltrazione dei dati possano essere usate per influenzare le politiche economiche e indebolire il processo decisionale degli Stati Uniti. Tali sviluppi hanno spinto il governo americano a intervenire con misure legislative specifiche, come la *Public Law* 118-50, che mira a proteggere i dati dei cittadini e a limitare l'influenza delle applicazioni digitali gestite da attori stranieri. Queste norme impongono, ad esempio, a piattaforme come TikTok di cedere il controllo o di vendere la piattaforma per ridurre il rischio che il governo cinese possa sfruttare i dati raccolti. L'influenza cinese, tramite la centralizzazione del controllo dei dati e la stretta collaborazione tra settore pubblico e privato, non solo permette di raccogliere informazioni vitali, ma anche di esercitare una forma di pressione strategica che può incidere direttamente sulle decisioni politiche ed economiche degli Stati rivali. Il futuro dello spionaggio informatico sarà caratterizzato da una crescente convergenza tra innovazione tecnologica e strategie di intelligence avanzate, dove la capacità di anticipare, monitorare e neutralizzare le minacce digitali diventa essenziale per mantenere la sicurezza nazionale. Le misure adottate dagli Stati Uniti per limitare l'influenza di piattaforme digitali cinesi, unitamente alla continua evoluzione delle tecnologie di raccolta e analisi dei dati, delineano uno scenario in cui la competizione tra grandi potenze si svolge sul terreno del cyberspazio, con implicazioni che vanno ben oltre la mera raccolta di

informazioni. Negli ultimi anni,[57] il panorama della sicurezza nazionale e delle operazioni di intelligence ha subito trasformazioni profonde, indotte sia da evoluzioni tecnologiche senza precedenti che da cambiamenti nell'assetto geopolitico globale. In questo contesto, il caso del dossieraggio in Italia emerge come un esempio emblematico e significativo, capace di fornire spunti fondamentali per comprendere le potenzialità e i rischi delle operazioni di cyberspionaggio del futuro. Il dossieraggio in Italia ha messo in luce come, in assenza di adeguati controlli e normative specifiche, la raccolta sistematica di informazioni personali e sensibili possa essere sfruttata per scopi di pressione e manipolazione politica. In quell'occasione, dossier dettagliati vennero utilizzati per monitorare, influenzare e persino distorcere il comportamento di soggetti e istituzioni critiche per l'assetto politico nazionale. Tale operazione ha evidenziato la vulnerabilità degli strumenti tradizionali di protezione dei dati e ha dimostrato che, senza un'efficace regolamentazione, le tecnologie di raccolta delle informazioni possono essere impiegate per scopi che vanno ben oltre la mera sicurezza nazionale, incidendo profondamente sulla fiducia dei cittadini e sulla stabilità delle istituzioni democratiche. Questo episodio italiano si inserisce in un quadro più ampio, in cui le piattaforme digitali e le tecnologie di sorveglianza stanno assumendo un ruolo centrale nello spionaggio informatico. Allo stesso modo in cui TikTok e altre applicazioni gestite da società con forti legami con il governo cinese hanno sollevato preoccupazioni a livello statunitense, il dossieraggio in Italia dimostra come anche in contesti europei vi siano pratiche di raccolta dati che, se non opportunamente regolate, possono essere utilizzate per influenzare il processo decisionale e per esercitare un controllo informativo invasivo. Il collegamento tra il caso italiano e gli scenari futuri dello spionaggio informatico è evidente: in un'epoca in cui la tecnologia permette la raccolta e l'analisi in tempo reale di enormi quantità di dati, il confine tra intelligence legittima e interferenze manipolative diventa sempre più labile. La capacità di accedere a informazioni sensibili, unita alla possibilità di utilizzarle per fini geopolitici, trasforma il cyberspionaggio in uno strumento non solo di raccolta, ma anche di potere e di influenza. Questo fenomeno, che si sta evolvendo in modo esponenziale, richiede una riflessione approfondita sul futuro delle operazioni di

[57] *C.Gallotti, Dossieraggio: bene la task force del Garante della privacy, 2024, cybersecurity360.it,*

intelligence, considerando la necessità di sviluppare sistemi di sicurezza avanzati e quadri normativi che possano contenere le derive manipolatorie. L'esperienza italiana ci insegna che è indispensabile un approccio multidisciplinare e integrato, che coniughi l'innovazione tecnologica con una rigorosa governance e con una normativa adeguata per garantire la protezione dei dati e la trasparenza nei processi di raccolta delle informazioni. Solo attraverso una strategia che unisca tecnologie avanzate, come l'intelligenza artificiale e il calcolo quantistico, a sistemi di controllo efficaci e a una cooperazione internazionale, sarà possibile contenere le potenzialità di abuso e le minacce che lo spionaggio informatico può comportare. L'esperienza del dossieraggio in Italia e le minacce derivanti dalla competizione con attori globali come la RPC sono solo alcuni dei segnali che indicano una trasformazione radicale in corso. Solo un approccio integrato, capace di unire innovazione tecnologica e regole di governance chiare, potrà garantire una gestione efficace delle sfide del futuro e tutelare la sicurezza nazionale in un'epoca dominata dal digitale.

# CONCLUSIONE

L'analisi condotta in questa tesi ha permesso di evidenziare come lo spionaggio informatico sia diventato una componente strategica essenziale nelle relazioni internazionali, ponendo sfide significative in termini di sicurezza, diritto e governance globale. Il cyberspazio rappresenta oggi il nuovo terreno di confronto tra Stati, attori non statali e organizzazioni criminali, con implicazioni che vanno ben oltre il semplice furto di informazioni riservate. L'assenza di un quadro normativo univoco e vincolante rende ancora più complesso il contrasto a tali fenomeni, sollevando interrogativi sulla protezione della sovranità statale, sulla fiducia reciproca tra gli Stati e sulla tutela dei diritti fondamentali dei cittadini.

Nel  Primo capitolo, l'analisi della normativa nazionale e internazionale ha mostrato come le attuali disposizioni giuridiche risultino spesso inadeguate a fronteggiare le minacce informatiche. Sebbene esistano strumenti normativi volti a regolamentare la sicurezza informatica e la protezione dei dati, la natura transnazionale dello spionaggio informatico richiede una cooperazione più efficace tra Stati e organismi sovranazionali. La frammentazione delle legislazioni e la mancanza di un quadro giuridico comune ostacolano un'azione coordinata e incisiva contro le attività di cyber-intelligence condotte a livello globale. Inoltre, la difficoltà di attribuire con certezza un attacco informatico a un determinato attore statale o non statale complica ulteriormente l'applicazione delle norme esistenti, creando una pericolosa zona grigia nel diritto internazionale.

Nel Secondo Capitolo, l'analisi dei casi di WikiLeaks, Datagate e del conflitto Russo-Ucraino ha messo in luce come lo spionaggio informatico possa avere ripercussioni dirette sulla stabilità internazionale, influenzando la fiducia tra gli Stati e ridefinendo le dinamiche geopolitiche. Il caso WikiLeaks ha evidenziato il conflitto tra il diritto all'informazione e la sicurezza nazionale, sollevando questioni etiche e giuridiche sulla trasparenza dei governi e sulla protezione delle fonti di intelligence. Il Datagate ha rivelato l'estensione delle operazioni di sorveglianza globale, mettendo in discussione il bilanciamento tra la sicurezza nazionale e la tutela della privacy individuale. Infine, lo spionaggio informatico nel conflitto russo-ucraino ha dimostrato come le guerre moderne si combattano sempre più anche nel cyberspazio, con operazioni mirate a destabilizzare

infrastrutture critiche, raccogliere informazioni sensibili e diffondere disinformazione su larga scala. Questo dimostra come il cyberspazio non sia solo un terreno di raccolta dati, ma anche un campo di battaglia dove si giocano equilibri strategici globali.

Nel Terzo Capitolo, l'attenzione si è concentrata sugli scenari futuri e sull'impatto dell'intelligenza artificiale nello spionaggio informatico. La crescente automazione dei processi di intelligence, resa possibile dalle nuove tecnologie, pone questioni etiche e giuridiche di grande rilievo. Il rischio di un utilizzo incontrollato dell'IA per la raccolta e l'analisi di dati sensibili solleva dubbi sulla responsabilità degli Stati e delle aziende tecnologiche, così come sulla necessità di sviluppare regolamentazioni efficaci per prevenire abusi. L'adozione di strumenti di machine learning avanzati e la capacità dell'IA di analizzare enormi volumi di dati in tempi ridotti rappresentano un'opportunità per migliorare le capacità difensive degli Stati, ma anche una minaccia per la privacy e i diritti individuali se utilizzati in modo indiscriminato.

Dall'analisi condotta emerge con chiarezza che il cyberspionaggio è destinato a diventare una delle principali sfide del XXI secolo. Per affrontare questa minaccia, sarà fondamentale un rafforzamento della cooperazione internazionale e l'adozione di normative più stringenti in grado di bilanciare le esigenze di sicurezza con la tutela dei diritti individuali. L'introduzione di meccanismi di attribuzione chiari e la creazione di protocolli condivisi tra Stati potrebbero costituire un passo avanti nella gestione dei conflitti cibernetici. Inoltre, la crescente dipendenza dalle tecnologie digitali rende necessario un ripensamento delle strategie di difesa informatica, sia a livello statale che privato. La creazione di standard globali condivisi e di organismi sovranazionali dedicati alla cybersecurity potrebbe rappresentare una soluzione efficace per regolamentare le attività di intelligence nel rispetto del diritto internazionale e della sovranità degli Stati. Non meno importante sarà il ruolo della diplomazia digitale, che dovrà assumere un peso crescente nel definire accordi tra Stati al fine di prevenire escalation derivanti da operazioni di spionaggio informatico.

In definitiva, lo spionaggio informatico continuerà a evolversi insieme alle tecnologie digitali, richiedendo risposte rapide e adeguate da parte della comunità internazionale. Solo attraverso una collaborazione globale, il rafforzamento della resilienza informatica e una regolamentazione chiara sarà possibile mitigare i rischi associati e garantire un equilibrio tra sicurezza, libertà e diritti fondamentali in un mondo sempre più interconnesso. L'importanza di un approccio multilivello, che combini innovazione tecnologica, strumenti giuridici e strategie diplomatiche, sarà determinante per affrontare le sfide future e proteggere la stabilità globale dalle minacce emergenti nel cyberspazio.

# Bibliografia


A, T. (2018). *Cyber espionage e cyber counterintelligence : spionaggio e controspionaggio cibernetico, Cyber Espionage e Cyber Counterintelligence.* Roma: Rubbettino Editore.

A.Calabrese. (2024). *L'applicazione del diritto umanitario alle operazioni cyber in guerra*. geopolitica.info.

*Analisi ISPI sull'estradizione di Assange e il cyberspionagigo* . (2024). ISPI Onilne.

*Annullare le accuse contro Julian Assange.* (2024). amnesty.it.

Benkler.Y. (2011). *Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate.* Harvard Law Review.

C.Gallotti. (2024). *Dossieraggio: bene la task force del Garante della privacy* . cybersecurity360.it.

Cistenrino, S. (2022). *Un nuovo uso della forza: la cyberwar nella guerra russo-ucraina* . scienzainrete.it.

Coleman.G. (2011). *Wikileaks: Whistleblowing in the Digital Age.* Journal of Indromation Technology & Policy.

*Ddl Cybersicurezza: così l'Italia rafforza le sue difese nel cyberspazio.* (2024). Agenda Digitale.

d'Europa, A. P. (s.d.). *Risoluzione 252, La Detenzione e la condanna di Julian Assange e i loro effetti sui diritti umani*.

D'Europa, C. (2015). *Risoluzione sulla sorveglianza di massa dell?NSA*.

E.Corsi. (2018). *La Nato a difesa del cyber spazio? Il dilemma nel diritto internazionale* . agendadigitale.eu.

Europea, C. (s.d.). *Legge sull'intelligenza artificiale.*

Europeo, P. (2014). *NSA,snooping: MEP's table proposals to protect EU citzens' privacy* .

F.Livelli. (2023). *Così l'intelligenza artificiale sta rivoluzionando la cyber security* .

F.Niola. (2024). *IA il primo trattato internazionale: la Convenzione del Consiglio d'Europa*. agendadigitale.eu.

F.Oliva. (2017). *Codice della privacy: cosa prevede?* www.informazionediscale.it.

F.Schifilliti. (2023). *Operazioni di cyberspionaggio nel conflitto Russo- Ucraino.* icttsecuritymagazie.com.

F.Sironi, D. G. (2019). *Il Manuale di Tallin* . www.cyberlaw.it.

Frattini. (2011). *Le nuove forme della diplomazia.* Dossier Lazio,intervista al ministro degli Affari Esteri.

group, M. (s.d.). *Il caso Tik Tok.* meridian-group.eu.

*Il ruolo dell'intelligenza artificiale per la sicurezza informatica.* (2024). cyberdivision.net.

J.D.Ohlin. (2015). *Cyber War: Law and Ethics for Virtual Conflicts*.

L.Di.Pietro. (2013). *Il manuale di Tallin: diritto e cyber war* . cesi-italia.org.

Ligustro, A. (2023). *Principio pacifista e uso della forza nel diritto intenrazionale contemporaneo.* Pescara: Convegno DPCE.

Lyon.D. (2015). *Surveillance after Snowden* . Polity Press.

M, F. (2017). *Shifting Meaning of Legal Certainty in Comparative and Transational Law* . Springer .

M.Cartisano. (2024). *Trattato globale Onu sulla Criminalità informatica*.

M.Kosinski. (2024). *Che cos'è l'hacking*. www.ibm.com.

M.Manzari. (2020). *La Convenzione di Budapest, L'Alba di una normativa di contrasto efficace al cybercrime*. Bari.

M.Santarelli. (2022). *NSA lo spionaggio del futuro e i nuovi equilibri geopolitici: le sfide*. agendadigitale.eu.

M.Tonellotto. (2020). *Criminalite cyberspazio, alcune riflesiioni in materia di cybercriminalità* . Bologna.

Maggio, J. (2024). *L'arte della guerra informatica*.

N.Ronzitti. (2013). *Datagate e le regole dello spionaggio*. formiche.net.

O.Terragni. (2025). *Cyberspionaggio Russo-Ucraina: tra campagne malware e copycat*. redhotcyber.com.

P.L.Bellia. (2012). *WikiLeaks and the Institutional Framework for National Security Disclosure*. The Yale Law Journal .

*Privacy Rights in the Digital Age*. (2013). aclu.org.

S, A. (2010). *The Impact of Wikileaks on Internazionale Security*. Journal of Cyber Policy .

S.Stefani. (2013). *Il caso Snowden e le conseguenze diplomatiche del Datagate*. Treccani.it.

T.Timm. (s.d.). *Cabelgate, One Year Later: How WikiLeaks has In*.

*The protection of privacy and personal data on the Internet and online media*. (2011). assembly.coe.int.

*Tutela della Sicurezza Pubblica vs Tutela della Privacy: un bilanciamento necessario*. (2020). diritto.it.

*Ucraina-Condanna degli attacchi russi che hanno colpito delle infrastutture civili* . (2024). it.ambafrance.org.

*UK sanctions cyber-crime gang it says Russia charged with attacking Nato*. (2024). reuters.com.

Unite, C. p. (s.d.). *Commento Generale n.16* . refworld.org.

Unite, R. d. (1970). *Dichiarazione relativa ai principi di diritto internazionale concernenti le relazioni amichevoli e la cooperazione tra gli Stati*.

V.Poitevin. (2024). *Il ricorso alla cyber nella cyberguerra Russo-Ucraina: analisi strategica si un esordio importante*. stormshiel.com.