CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

CYBERSECURITY: UNA SFIDA TRA PUBBLICA SICUREZZA E SICUREZZA NAZIONALE

Il presente elaborato si propone lo scopo di evidenziare le sempre crescenti interrelazioni tra la tematica della cybersecurity e quelle di Pubblica Sicurezza e Sicurezza Nazionale. Segnatamente, verranno esaminati dal punto di vista teorico i predetti concetti di Pubblica Sicurezza, Sicurezza Nazionale e Sicurezza Cibernetica e, in seguito, verranno illustrati i rischi per l'ordine pubblico e la difesa nazionale derivanti dagli attacchi informatici. Inoltre, si illustreranno le competenze degli organismi istituzionalmente deputati alla tutela della cybersecurity in Italia e, infine, sarà analizzata la legislazione nazionale e sovranazionale vigente in materia, con particolare riferimento al perimetro di sicurezza nazionale cibernetica.

di **Vittorio Guarriello**
IUS/09 - ISTITUZIONI DI DIRITTO PUBBLICO
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Venerdì 25 Febbraio 2022

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

The purpose of this paper is to highlight the ever-growing interrelationships between cybersecurity and Public Security and National Security. In particular, the above-mentioned concepts of Public Security, National Security, Cybernetic Security will be examined from a theoretical point of view and, then, it will be illustrated the risks to public order and national defence arising from cyber attacks. Moreover, it will be explained the competences of the bodies institutionally responsible for the protection of cybersecurity in Italy and, finally, it will be analyzed the national and supranational legislation in force in this area, with particular reference to national cybernetic security perimeter.

---

1. Introduzione

La costante e crescente evoluzione tecnologica, come è noto, ha comportato profondi mutamenti sia in tutti gli aspetti della vita quotidiana delle persone[1] sia, più in generale, nelle attività e nei settori d'interesse degli apparati statali.

Nondimeno, tale fenomeno ha comportato la necessità dell'approntamento di sempre più incisivi ed efficaci strumenti di contrasto alle azioni poste in essere mediante strumenti informatici, suscettibili di ledere o porre in pericolo la sicurezza dei singoli individui o degli Stati.

La peculiarità del web, difatti, è quella che, pur essendo connotato da immaterialità, il suo utilizzo ha moltissimi risvolti afferenti alla sicurezza dei cittadini e delle Istituzioni.

Invero, in virtù della quantità di risorse contenute all'interno del world wide web ci troviamo oggi al cospetto di un vero e proprio "spazio digitale" (detto anche "cyberspazio"), inteso come lo spazio virtuale nel quale utenti e programmi connessi fra loro mediante una rete telematica, interagiscono e comunicano fra loro per finalità diverse (es. consultazione di banche dati o scambio di messaggi di posta elettronica), da cui, però, possono derivare rischi estremamente concreti.

CamminoDiritto.it
ISSN 2421-7123

Infatti, all'interno della rete internet sono contenuti tantissimi dati ed informazioni, anche sensibili, riguardanti ciascun individuo e, mediante i servizi online offerti dagli istituti bancari, i titolari di conto corrente possono disporre costantemente del capitale ivi depositato.

In conseguenza di ciò, le informazioni di carattere personale, professionale ed economico (la c.d. "identità digitale") risultano essere in qualche modo affiancate e sovrapposte all'identità personale del singolo.

Per di più, a cagione dell'implementazione delle tecnologie digitali, anche le Pubbliche Amministrazioni hanno modificato il proprio modo di operare, fondando sempre di più le loro attività sull'utilizzo di sistemi informatici, anche in settori particolarmente sensibili, quali, ad esempio, la sanità, i trasporti e l'aviazione civile.

Sfortunatamente, al pari di qualsivoglia evento della storia umana, anche dallo sviluppo delle tecnologie digitali sono scaturite ripercussioni negative e fattori di criticità.

Difatti, i sodalizi criminali hanno colto le potenzialità offerte dagli strumenti tecnologici in ordine alla possibilità di realizzare con maggior rapidità e su più larga scala le loro attività illecite.

Allo stesso modo, oramai molto spesso anche singoli malintenzionati attuano varie tipologie di reati adoperando mezzi digitali (truffe, frodi informatiche, stalking), aumentandone, in alcuni casi, gli effetti lesivi e riuscendo a colpire vittime residenti anche in luoghi geograficamente molto distanti da loro.

Ebbene, per tali ragioni, appare evidente come sia lo spazio digitale nel suo complesso, sia le singole identità digitali e le attività realizzate online dai cittadini necessitino di sempre più efficaci forme di tutela.

Invero, la tematica della sicurezza cibernetica, lungi dall'essere un argomento settoriale e di interesse esclusivamente per specialisti del settore informatico, rappresenta una problematica di enorme rilevanza per la sicurezza dei singoli cittadini, ma anche degli apparati statali.

Infatti, a cagione del sopradescritto diffuso e consolidato utilizzo delle reti informatiche sia da parte degli individui che delle Pubbliche Amministrazioni, le questioni della cybersicurezza intersecano sempre di più, come si vedrà nel prosieguo della trattazione,

CamminoDiritto.it
ISSN 2421-7123

quelle inerenti la Pubblica Sicurezza e la Sicurezza Nazionale ed hanno assunto un tale rilievo che alcuni osservatori si sono interrogati sulla possibilità di considerarla un vero e proprio bene pubblico[2] .

2. La Pubblica Sicurezza

Il concetto di Pubblica Sicurezza, pur essendosi evoluto nel corso del tempo anche in ragione dei mutamenti sociali e dei cambiamenti delle forme di Stato, ha un fondamento che è rimasto tendenzialmente costante, ossia il fine di garantire l'ordinato e tranquillo svolgimento della vita sociale, sintetizzato nel brocardo latino ne cives ad arma ruant[3].

In altre parole, lo scopo a cui tendono le attività di tutela della Pubblica Sicurezza è quello di prevenire e contrastare le attività e le condotte suscettibili di arrecare turbamento alla convivenza civile, affinché esse non costituiscano la scaturigine di reazioni violente da parte di singoli individui o gruppi di cittadini.

Sotto il profilo oggettivo, il bene tutelato dall'attività di Pubblica Sicurezza (o Polizia di Sicurezza) è tradizionalmente individuato nell'ordine pubblico[4], da intendersi – secondo la definizione elaborata dalla dottrina nell'ambito degli studi in materia di Diritto Costituzionale e Pubblico – quale l'insieme dei "principi etici e politici, la cui osservanza ed attuazione sono ritenute indispensabili all'esistenza di tale ordinamento ed al conseguimento dei suoi fini essenziali" (ordine pubblico c.d. "ideale") [5] e come "il buon assetto o il regolare andamento del vivere civile, a cui corrispondono, nella collettività, l'opinione e il senso della tranquillità e della sicurezza" (ordine pubblico c.d. "materiale") [6].

Accedendo a tale orientamento, quindi, la Pubblica Sicurezza è da intendersi come l'integrità fisica e patrimoniale dei privati che, qualora pregiudicata da condotte lesive, rileverebbe come danno per la collettività nel suo complesso, pur riguardando esclusivamente dei singoli. Ciò proprio perché le lesioni dell'incolumità fisica o del patrimonio dei privati possono mettere a repentaglio sia l'ordinato svolgersi del vivere civile il senso della tranquillità e della sicurezza in seno alla pubblica opinione.

Con maggiore impegno esplicativo, accedendo a tale opzione esegetica la Pubblica Sicurezza rappresenta la pratica estrinsecazione del concetto di ordine pubblico materiale sotto il profilo della tutela dei privati.

A sua volta, secondo parte della dottrina, le due suesposte accezioni di ordine pubblico sono tra loro poste in un rapporto di strumentalità, vale a dire che mediante il

CamminoDiritto.it
ISSN 2421-7123

mantenimento dell'ordine pubblico materiale, viene tutelato l'ordine pubblico ideale[7].

Dunque, ad avviso di tale opinione i termini ordine pubblico e sicurezza pubblica sarebbero dicotomici, mantenendo due significati distinti e concettualmente differenti.

Nondimeno, la sopra illustrata accezione dei concetti di ordine pubblico e Pubblica Sicurezza è stata rimeditata a seguito dell'entrata in vigore della Costituzione.

Segnatamente, si è cominciato a dubitare che nell'ambito del nostro ordinamento costituzionale potesse ancora rinvenirsi una siffatta concezione di ordine pubblico in senso ideale.

Tale impostazione critica si fonda sul rilievo che la nostra Carta Costituzionale pone taluni limiti ai diritti inviolabili del cittadino all'uopo di tutelare l'ordine pubblico, sicché rappresenterebbe una contraddizione in termini, ritenere che al fine di tutelare il sistema fondamentale di valori e principi dell'ordinamento vengano poste delle limitazioni a diritti che sono la trasposizione sul piano pratico, proprio dei cennati principi.

Pertanto, la dottrina più moderna ritiene che la nostra Grundnorm prenda in considerazione l'ordine pubblico prettamente sotto il suo profilo materiale, identificando, di conseguenza, la Pubblica Sicurezza come l'attività tesa a garantire la tranquillità sociale.

Il suesposto orientamento è stato, in tempi non risalenti, confermato dal legislatore che all'art.159 co.2 d.lgs. 112/1998 ha definito l'ordine pubblico come "complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle Istituzioni, dei cittadini e dei loro ben" e la Pubblica sicurezza come l'insieme delle "e misure preventive e repressive dirette al mantenimento dell'ordine pubblico". Anche la Corte Costituzionale si è espressa in tal senso, definendo la Pubblica Sicurezza come attinente "alla funzione inerente la prevenzione dei reati o al mantenimento dell'ordine pubblico" [8].

Ebbene, tale opzione esegetica ritiene, quindi, che i termini ordine pubblico e Pubblica Sicurezza costituiscano una vera e propria endiadi, afferendo allo stesso ambito concettuale ed essendo tra loro inestricabilmente complementari.

Alla luce delle considerazioni innanzi svolte, appare evidente come la tematica della sicurezza informatica assuma un fondamentale rilievo in relazione alla tutela della Pubblica Sicurezza.

CamminoDiritto.it
ISSN 2421-7123

Difatti, la crescente diffusione dei reati informatici[9] – che, come risaputo, sono connotati da caratteristiche di pervasività ed invasività, in ragione dell'aspazialità propria delle tecnologie digitali - certamente mette in pericolo l'integrità dei singoli individui e del loro patrimonio, con conseguenti, possibili, ripercussioni alla percezione della sicurezza in seno alla pubblica opinione.

3. La Sicurezza Nazionale

La Sicurezza Nazionale è un concetto di non agevole definizione, tanto che un autore ne ha parlato come un simbolo ambiguo, suscettibile di assumere moltissimi significati diversi, con il conseguente rischio di non assumere alcun significato concreto [10].

In linea di principio, può essere definita – secondo gli approdi dottrinali più moderni – come la tutela dei vari interessi nazionali (nei singoli settori) che assumono rilievo in relazione alla sua indipendenza politica, integrità territoriale e coesione socio-politica[11].

Difatti, essa viene, talvolta, rappresentata graficamente come l'area d'intersezione tra più cerchi, ciascuno dei quali rappresentativo dell'interesse politico – militare, di quello energetico e di quello economico (c.d. catena della sicurezza).

Il più importante contributo alla normativizzazione del concetto in esame – invero già citato dall'art. 126 Cost., a tenore del quale lo scioglimento della Giunta regionale e la rimozione del Consiglio possono essere disposti dal Presidente della Repubblica quando, tra l'altro, lo impongano ragioni di sicurezza nazionale – è stato apportato ad opera della {https/URL}[12], recante la riforma del sistema d'informazione per la sicurezza della Repubblica.

Difatti, dall'esegesi della suddetta legge la sicurezza Nazionale può essere definita come l'insieme delle attività a tutela della difesa dell'indipendenza, dell'integrità e della sicurezza statale funzionali <<alla protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia>>.

Giova precisare che il concetto di sicurezza nazionale non deve essere confuso né con quello affine di difesa nazionale – che, invece, riguarda le attività poste a presidio dell'indipendenza dello Stato e la reazione nei confronti di minacce esterne – né, tantomeno, con quello di Pubblica Sicurezza delineato nel precedente paragrafo.

Orbene, alla luce di tale definizione si comprende come anche il tema della cybersecurity

CamminoDiritto.it
ISSN 2421-7123

risulti essere rilevante anche in relazione alla Sicurezza Nazionale.

Invero, qualora azioni di sabotaggio o di furto di dati abbiano ad oggetto infrastrutture critiche di rilevanza nazionale (ad es. strutture sanitarie, centri strategici nel sistema dei trasporti o dell'approvvigionamento energetico, centri di ricerca di rilevanza nazionale) o enti ed Istituzioni centrali, è evidente come esse risultino lesive proprio degli interessi politici, militari, economici, scientifici ed industriali che costituiscono il nucleo concettuale della Sicurezza Nazionale.

Non è, poi, trascurabile la circostanza che ad oggi anche talune azioni finalizzate al raggiungimento di scopi militari vengono poste in essere nel cyberspazio. Trattasi della c.d. cyberwar o cyberwarfare, definita da qualche esperto come la forma di belligeranza tipica della terza rivoluzione industriale[13].

Segnatamente, le azioni di guerra cibernetica possono sostanziarsi nell'attacco ad infrastrutture critiche, nell'intercettazioni di dati e conversazioni rilevanti oppure nel sabotaggio e/o nell'intralcio alle apparecchiature militari o di pubblica utilità basate su tecnologie informatiche o satellitari.

Più nel dettaglio, tali tipologie di attacchi possono essere perpetrati a livello fisico (ossia, distruggendo materialmente gli apparati informatici presi a bersaglio), sintattico (cioè, attaccando i sistemi computerizzati mediante armi informatiche, quali trojan e spyware al fine di infiltrarvisi; attacchi DoS (Denial of Service) tesi a rendere inservibili le infrastrutture tecnologiche dell'avversario e virus e cryptolocker (all'uopo di cancellare tutte le informazioni memorizzate nell'hard disk) oppure semantico, vale a dire condizionando gli avversari – adoperando tecniche di ingegneria sociale – al fine di porre in essere azioni di phishing ed impossessarsi di informazioni riservate o credenziali d'accesso ai sistemi informatici.

Dunque, l'approntamento di efficaci strumenti di tutela della sicurezza cibernetica rientra pienamente anche nel mantenimento di un'efficiente capacità militare dello Stato.

4. La sicurezza cibernetica

In linea di prima approssimazione, la sicurezza cibernetica può essere definita – secondo autorevoli studi in materia – come l'attività tesa alla protezione dei sistemi informatici e delle informazioni dagli stessi trattate da potenziali rischi e violazioni[14].

Segnatamente, dal punto di vista tecnico le azioni finalizzate alla tutela della sicurezza

CamminoDiritto.it
ISSN 2421-7123

cibernetica agiscono, nella gran parte dei casi, su un triplice piano: logico, fisico e funzionale all'uopo di garantire la disponibilità dei sistemi e delle informazioni solo in favore dei soggetti autorizzati (riservatezza), la difesa della completezza delle informazioni (integrità) e la costante possibilità di accesso e di utilizzo alle informazioni ed ai sistemi da parte dei soggetti autorizzati (disponibilità) .

Più nel dettaglio, si cerca di tutelare la sicurezza dei sistemi informatici a livello fisico allocando i server in luoghi sicuri e sorvegliati. Inoltre, si agisce a livello logico, prevedendo la possibilità di utilizzo dei sistemi esclusivamente da parte di utenti autorizzati mediante autenticazione e individuando diversi livelli di sicurezza degli utenti, in ragione della quantità e/o della qualità di informazioni delle quali possono prendere cognizione.[15]

Ancora, la protezione dagli attacchi informatici avviene anche a livello funzionale, effettuando monitoraggi delle attività poste in essere nei sistemi dagli utenti autorizzati all'accesso e mediante l'utilizzo di file di log finalizzati al tracciamento ed alla registrazione di tali attività (c.d. accountability).

Sotto altro profilo concettuale, poi, gli esperti del settore sono soliti effettuare una distinzione tra misure di sicurezza passiva – cioè quelle tese alla difesa dei sistemi dall'accesso di utenti non autorizzati e che, solitamente, agiscono sul piano fisico e logico – e misure di sicurezza attiva, vale a dire quelle finalizzate a rendere le stesse risorse contenute nei sistemi intrinsecamente sicure e protette, di talché anche qualora un utente non autorizzato riesca ad accedere al sistema informatico, non riesca, poi, a prenderne cognizione .

Dal punto di vista giuridico, a differenza dei reati informatici e delle azioni poste in essere dagli hacker che interessano da tempo l'opera del legislatore ed il dibattito degli esperti, il concetto di sicurezza cibernetica ha fatto ingresso da poco tempo nella legislazione.

In particolare, il cennato concetto è stato introdotto nell'ordinamento giuridico ad opera di vari provvedimenti normativi (nel dettaglio, DPCM 17 Febbraio 2017; D.Lgs. 65/2018 che ha recepito la direttiva 2016/1148 c.d. direttiva NIS; e, da ultimi, il D.L. 105/2019 ed il DPCM 131/2020).

Nello specifico, i citati D.L. 105/2019 – recante misure afferenti alla protezione dello spazio cibernetico - ed il DPCM 131/2020 adottato all'uopo di limitare l'utilizzo di infrastrutture tecnologiche nell'approntamento della costituenda rete 5G italiana, anche mediante l'utilizzo del c.d. golden power da parte del Presidente del Consiglio dei Ministri - tutela le infrastrutture tecnologiche utili al "mantenimento di attività civili,

CamminoDiritto.it
ISSN 2421-7123

sociali o economiche fondamentali per gli interessi dello Stato" - individuando, quindi, settori d'interesse analoghi a quelli afferenti ai concetti di ordine e sicurezza pubblica, come delineati dalla sopracitata giurisprudenza costituzionale.

Inoltre, appare evidente che il concetto in esame afferisca anche all'ambito della Difesa dello Stato.

Pertanto, deve ritenersi che la sicurezza nazionale cibernetica, non costituisca un concetto autonomo rispetto a quelli di ordine e sicurezza pubblica e sicurezza nazionale, ma sia ad essi trasversale, costituendone un settore tecnico[16].

5. I rischi per la Pubblica Sicurezza e la Sicurezza Nazionale derivanti da attacchi informatici

Il principale pericolo per la Pubblica Sicurezza scaturente dalle tecnologie informatiche è rappresentato dall'utilizzo distorto delle stesse da parte delle organizzazioni criminali tradizionali, al fine di massimizzare i profitti ed ampliare i loro illeciti settori d'azione e dalla circostanza che nuovi gruppi delinquenziali, o singoli individui, abbiano scelto quale settore d'elezione la commissione di reati informatici.

Invero come è noto, purtroppo le potenzialità offerte dalle nuove tecnologie vengono sfruttate sempre di più da organizzazioni criminali e malintenzionati che hanno colto, sin da subito, la possibilità di utilizzarle al fine di agevolare lo svolgimento dei loro traffici illeciti e di compiere nuove tipologie di reati, forieri di lucrose occasioni di guadagno.

Segnatamente, lo sviluppo del web ha consentito sia alle consorterie criminali maggiormente capaci di intercettare i cambiamenti in atto di incrementare notevolmente i margini di profitto, aumentandone la pericolosità, sia a nuovi gruppi criminali o a singoli – anche non legati a sodalizi delinquenziali – di "specializzarsi" nel compimento di reati informatici.

Difatti, la Direzione Nazionale Antimafia in un proprio recente report, ha evidenziato il crescente utilizzo da parte della criminalità organizzata tradizionale di servizi online a fini di riciclaggio di denaro, in ragione della semplicità con cui è possibile, mediante essi, trasferire capitali nei paradisi fiscali.

Inoltre, è stato accertato un frequente uso da parte della criminalità di criptovalute, - quali Bitcoin, Ethereum, Diem - come mezzo di pagamento nell'ambito di attività illegali, atteso che risultano estremamente difficoltosi – a cagione dell'inesistenza di enti

CamminoDiritto.it
ISSN 2421-7123

intermediari – l'identificazione dei soggetti della transazione e l'esecuzione di sequestri patrimoniali.

Ancora, alcune delle più diffuse applicazioni di messaggistica istantanea, quali Telegram, Viber, Whatsapp e Surespot, adoperano particolari algoritmi crittografici, tali da renderli difficilmente intercettabili dagli apparati investigativi.

Inoltre, ulteriore fattore di criticità è rappresentato dalla nascita di sodalizi criminali emergenti, sovente dotati di elevatissime competenze tecniche nel settore informatico.

Al riguardo, varie Forze di Polizia hanno ipotizzato che moltissimi attacchi informatici posti in essere su larga scala e furti di dati sensibili ai danni di multinazionali o agenzie governative siano stati posti in essere da gruppi organizzati di hackers, operanti in una dimensione di transnazionalità.

Oltre a ciò, è d'uopo evidenziare che nelle more dell'emergenza epidemiologica da COVID – 19, moltissimi individui, tra cui anche soggetti dediti ad attività illecite, hanno acquisito maggiore praticità nell'utilizzo delle tecnologie informatiche, in ragione della moltitudine di attività che sono state svolte sul web durante tale periodo, sicché il numero di reati informatici è verosimilmente destinato ad aumentare.

Infine, alcuni analisti hanno evidenziato con preoccupazione il diffuso utilizzo dell'applicazione di messaggistica istantanea denominata Telegram a fini illegali.

Infatti, tale applicazione risulta essere di intuitivo utilizzo ma, grazie all'utilizzo della crittografia end to end[17], assicura notevole riservatezza ai suoi utenti, rendendo possibile la commissione di reati informatici, anche particolarmente gravi (es. pedopornografia o traffici di sostanze illegali) a soggetti anche non in possesso di particolari competenze tecniche.

Inoltre, l'applicazione Telegram è stata di recente individuata da alcune operazioni di Polizia Giudiziaria anche quale canale utilizzato per la vendita di Green Pass falsi.

Sotto il profilo dei rischi per la Sicurezza Nazionale, invece, deve essere in primo luogo evidenziato il fenomeno del cyberterrorismo, consistente nell'utilizzo del world wide web da parte di organizzazioni terroristiche a fini di propaganda, scambio di informazioni e pianificazioni di attentati, nonché nella commissione di attacchi hacker volti alla distruzione o al deterioramento di sistemi informatici di rilevanza nazionale.

CamminoDiritto.it
ISSN 2421-7123

Inoltre, rappresentano sicuramente un rilevante rischio per la Sicurezza Nazionale tutti i furti di dati e gli attacchi hacker tesi al danneggiamento di infrastrutture critiche posti in essere da uno Stato ai danni di un altro.

Nel corso di alcune operazioni, è stato adoperato il virus informatico noto come Stuxnet, teso ad inibire il funzionamento di alcuni componenti delle centrali nucleari, in particolar modo le centrifughe, e capace di autoreplicarsi su altri dispositivi.

Un'altra vicenda paradigmatica della pericolosità del cybercrime per la Sicurezza Nazionale e la Pubblica Sicurezza è quella divenuta nota mediaticamente come "Caso Occhionero" ed afferente ad un'attività di cyberspionaggio posta in essere da due ingegneri informatici a danno di svariate personalità di spicco delle Istituzioni, ma soprattutto di enti pubblici aziende private, operanti in settori strategici (uno su tutti, l'Ente Nazionale per l'Aviazione Civile).

Difatti, la Procura della Repubblica presso il Tribunale Ordinario di Roma contestava loro, in alcuni capi di imputazione, di aver carpito "notizie che nell'interesse politico interno o della sicurezza pubblica devono rimanere riservate e di cui in ogni caso vietata la divulgazione ovvero dati personali e sensibili relativi ad intestatari ed utilizzatori dei sistemi informatici e telematici violati" e di aver provato ad accedere ad un sistema informatico [18].

Al riguardo, il Giudice per le Indagini Preliminari che ha applicato nei confronti dei due indagati la misura cautelare personale della custodia cautelare in carcere, nel motivare l'adozione del provvedimento restrittivo della libertà personale maggiormente afflittivo, ha evidenziato come gli stessi fossero riusciti addirittura a venire a conoscenza del procedimento penale instaurato a loro carico e stessero ponendo in essere un'attività di inquinamento probatorio.

Ebbene, tutte le considerazioni innanzi svolte ci consentono di comprendere come, sotto il profilo pratico, la cybersicurezza rientri a pieno titolo tra i settori d'interesse degli apparati statali al fine di salvaguardare le proprie Istituzioni e contrastare i fenomeni criminali.

6. Gli organismi istituzionalmente deputati alla Tutela della Cybersecurity in Italia

Il fenomeno non ha ovviamente lasciato indifferenti le Istituzioni che hanno, nel corso del tempo, istituito svariati organismi di contrasto.

CamminoDiritto.it
ISSN 2421-7123

Segnatamente, si è avuta l'istituzione di Reparti delle Forze dell'Ordine e delle Forze Armate competenti in materia ed una sempre maggiore specializzazione degli stessi.

Per quanto attiene alle Forze dell'Ordine, la Polizia di Stato opera in tale settore principalmente per il tramite della Polizia Postale e delle Comunicazioni, alle dipendenze della quale è posto il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAICIP), competente in merito alla prevenzione e della repressione dei Computer Crimes, volti al danneggiamento delle infrastrutture informatizzate di natura critica e di rilevanza nazionale.

Inoltre, di recente, vi è stata l'istituzione presso il Dipartimento della Pubblica Sicurezza la Direzione Centrale per la polizia scientifica e la sicurezza cibernetica, deputata, tra i vari compiti ad essa demandati, alla gestione del Cert (Computer Emergency Response Team), vale a dire il centro di supporto dei sistemi di sicurezza informatica e cibernetica del Ministero dell'Interno.

La Guardia di Finanza opera in materia mediante un reparto specializzato, ossia il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, deputato al contrasto del cybericiclaggio, del contrabbando, del gioco d'azzardo illegale e, più in generale, di tutti i traffici illeciti commessi via web, nonché al costante monitoraggio della rete al fine di sviluppare attività investigative, qualora vengano individuate indizi sintomatici di attività illecite in materia economico – finanziaria poste in essere sul web.

L'Arma dei Carabinieri ha, invece, istituito presso il Raggruppamento Carabinieri Investigazioni Scientifiche il Reparto Tecnologie Informatiche, la cui articolazione è basata su tre sezioni (elettronica, informatica e cibernetica), deputato ad effettuare indagini nel settore della Digital forensics ed alla soddisfazione di esigenze di ricerca nel settore delle tecnologie informatiche.

Con riferimento, invece, alle Forze Armate l'Esercito Italiano si è dotato di un apposito Reparto Sicurezza Cibernetica, alle cui dipendenze e posto personale specializzato in ambito informatico e capace di pianificare ed eseguire tutte le attività in materia di cyber defence.

Parimenti, sono istituiti presso gli stormi dell'Aeronautica Militare apposite Computer Incident Response Team, chiamati a gestire ed a risolvere le situazioni di emergenze derivanti da attacchi informatici, ed esiste un Centro Operativo Cibernetico nell'ambito del Reparto Sistemi Informativi Automatizzati, con compiti di protezione delle reti informatiche della Forza Armata ed analisi delle minacce.

CamminoDiritto.it
ISSN 2421-7123

La Marina Militare ha istituito presso il proprio Stato Maggiore un Ufficio Sicurezza Cibernetica, Informatica e delle Comunicazioni, alle cui dipendenze è posta la sezione cyberdefence avente compiti di prevenzione degli attacchi informatici e di risoluzione di eventuali incidenti.

Ancora, presso lo Stato Maggiore della Difesa operano il Comando Operazioni in Rete, con funzioni di coordinamento di tutte le attività del dicastero della Difesa in rete, e di supervisione delle attività di cybersecurity del predetto Ministero e le Cellule operative cibernetiche, ossia team interforze di specialisti, proiettabili anche all'estero, tra i cui compiti assume precipuo rilievo la difesa delle infrastrutture militari dalle minacce cibernetiche .

Da ultimo, deve segnalarsi l'istituzione - ad opera del D.L. 82/2021, convertito con modificazioni in l. 109/2021 - dell'Agenzia Nazionale per la Cybersecurity con compiti di coordinamento delle attività in materia di tutte le Pubbliche Istituzioni; di sviluppo della prevenzione nell'ambito della sicurezza cibernetica e di presidio degli interessi nazionali in tale settore. Inoltre, tale Agenzia è stata designata quale Autorità Nazionale in materia di cybersicurezza.

7. Brevi cenni su PNRR e Sicurezza Cibernetica

Una testimonianza del ruolo che ha assunto la sicurezza cibernetica nell'ambito delle politiche statali è fornita dalla circostanza che essa sia stata espressamente presa in considerazione dal Piano Nazionale di Ripresa e Resilienza, ossia il programma di investimenti ed interventi, elaborato al fine di rilanciare l'economia italiana a seguito della crisi economica derivante dall'emergenza epidemiologica da COVID – 19.

In disparte, quanto previsto in relazione all'ammodernamento tecnologico delle imprese private, difatti, la sicurezza cibernetica rappresenta il primo dei sette investimenti previsti per la Digitalizzazione della P.A., che è uno degli obiettivi principali della componente "Digitalizzazione, innovazione e sicurezza nella PA", a sua volta ricompresa nella missione "Digitalizzazione, innovazione, competitività, cultura e turismo".

Più nello specifico, il piano prevede uno stanziamento di 7 miliardi e 950 milioni di euro finalizzato allo sviluppo di infrastrutture connotate da alta affidabilità ed efficienza per la fornitura di servizi cloud alla Pubblica Amministrazione.

Segnatamente, tali tecnologia dovranno rispettare gli standard minimi di sicurezza definiti dall'AGID e le misure attuative della direttiva c.d. NIS.

CamminoDiritto.it
ISSN 2421-7123

Inoltre, nell'ambito di tale intervento, il piano si pone quale obiettivo l'interoperabilità tra le varie banche dati in uso alle singole Pubbliche Amministrazioni, all'uopo di superare le criticità derivanti dall'utilizzo di plurimi CED (Centri Elaborazione Dati), anche al fine di garantire una maggiore sicurezza delle informazioni e delle risorse ivi contenute.

Giova precisare che i due suesposti interventi risultano essere tra loro interconnessi.

Difatti, l'obiettivo finale che il Governo si è proposto, in linea con l'EU Data Strategy, è quello di giungere alla creazione di una sorta di "Sistema Operativo del Paese", ossia la creazione di un cloud , sicuro ed affidabile, reso fruibile mediante un catalogo API (Application Programminig Interface), all'interno del quale sono contenuti tutti i dati e le informazioni in possesso delle Pubbliche Amministrazioni ed a cui le singole PA, centrali e periferiche, possano accedere – in ragione del livello di autorizzazione posseduto – allo scopo di elaborarli per poter, poi, fornire servizi adeguati a cittadini ed imprese[19].

Tali provvedimenti, si pongono nel solco di una sempre maggiore attenzione nei confronti dell'informatizzazione e della modernizzazione della PA, nella consapevolezza che ciò rappresenta uno dei pilastri fondamentali per la creazione di un Sistema Paese efficiente.

8. Il Perimetro di Sicurezza Nazionale Cibernetica.

Il principale provvedimento assunto in materia di Cybersecurity è rappresentato, però, dall'istituzione del Perimetro di Sicurezza Nazionale Cibernetica.

La scaturigine di tale provvedimento è da rinvenirsi a livello comunitario nella direttiva UE 2016/1148 (c.d. Direttiva NIS), finalizzata espressamente all'implementazione di un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea" ed a livello nazionale nella {https/URL}#160;2017 che hanno modulato una vera e propria architettura cyber dello Stato[20].

L'attuazione della citata direttiva nell'ordinamento giuridico italiano è avvenuta ad opera del D.L. 105/2019, convertito con modifiche nella legge 18 novembre 2019 num.133, ai sensi del quale è stato formalmente istituito il Perimetro di Sicurezza Nazionale Cibernetica.

In seguito il DPCM numero 131 del 30 luglio 2020 ha enucleato i criteri in basi ai quali individuare i soggetti da includere nel perimetro di sicurezza cibernetica.

CamminoDiritto.it
ISSN 2421-7123

In sintesi, l'insieme delle disposizioni che è possibile ricavare dai tre suesposti provvedimenti legislativi – oltre a definire taluni rilevanti concetti in materia, quali "rete", "sistema informativo", "servizio informatico" "bene ICT" e "architettura e componentistica" - individua una serie di soggetti tra gli esercenti una funzione fondamentale dello Stato o che prestano un servizio essenziale per gli interessi dello Stato, la cui compromissione rappresenterebbe una problematica rilevante in ordine alla Sicurezza Nazionale[21].

Inoltre, ai sopraelencati soggetti governativi si aggiungono quelli privati operanti nei settori della difesa, dello spazio e aerospazio, dell'energia, delle telecomunicazioni, dell'economia e finanza, dei trasporti, dei servizi digitali, delle tecnologie critiche, degli enti previdenziali e del lavoro[22].

Tutti i sopraelencati soggetti sono tenuti ad adottare specifiche misure volte a garantire elevati livelli di sicurezza, relative a tutta la gestione del processo della sicurezza delle informazioni ed a comunicare alle autorità preposte gli incidenti informatici che li vedono coinvolti.

Inoltre, i soggetti ricompresi nel perimetro di sicurezza cibernetica debbono predisporre ed aggiornare, trasmettendolo alla Presidenza del Consiglio dei ministri, un elenco delle risorse informatiche a loro in uso, individuando quelli necessari all'assolvimento delle loro funzioni e quelli che, in caso di incidente, comporterebbero l'interruzione, totale o parziale, delle loro attività.

Tra i vari organi, la normativa in materia di perimetro di sicurezza cibernetica – oltre alla già citata Agenzia Nazionale per la Cybersecurity avvenuta nel 2021 - istituisce anche il Centro di Valutazione e Certificazione Nazionale (CVCN) in seno al Ministero dello sviluppo economico, cui è demandato il compito di effettuare la valutazione di beni, sistemi e servizi informatici destinati ad essere impiegati su infrastrutture ICT, che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato, i Centri di Valutazione Acquisti (CEVA) accreditati presso il Ministero della Difesa e dell'Interno ed il Nucleo per la sicurezza cibernetica (NSC), posto alle dipendenze del Dipartimento delle informazioni per la sicurezza, cui sono demandate attività in materia di prevenzione, preparazione e gestione delle crisi cibernetiche.

Ancora, sono previste specifiche procedura in materia di acquisto di beni ICT da parte delle Pubbliche Amministrazioni.

CamminoDiritto.it
ISSN 2421-7123

Invero, l'art. 1 co.6 {https/URL}(CVCN), indicando, altresì, la valutazione del rischio associato all'oggetto della fornitura, anche in base al settore di utilizzo.

Tale Centro di Valutazione ha la possibilità di effettuare verifiche preliminari ed imporre condizioni e test sull'hardware e sul software, nel termine di quarantacinque giorni dalla ricezione della comunicazione, prorogabile una sola volta per giorni quindi nei casi connotati da particolare complessità.

Decorso il termine di 45 giorni senza che il CVCN si sia pronunciato, l'ente che ha effettuato la comunicazione può procedere nell'affidamento.

Nell'ipotesi in cui, invece, il predetto organismo imponga delle condizioni o dei test, sia per l'hardware che per il software, il bando di gara e il contratto dovranno contenere specifiche clausole che condizionano, sospensivamente o risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN, che devono comunque essere conclusi nel termine di sessanta giorni.

Decorso il suddetto termine, la pubblica amministrazione o la centrale di committenza che ha effettuato la comunicazione ha facoltà di procedere nell'assegnazione dell'affidamento In deroga a quanto sopra stabilito, è espressamente sancito che non sono oggetto di comunicazione gli affidamenti delle forniture di beni, sistemi e servizi ICT destinate alle reti, ai sistemi informativi e ai servizi informatici utili allo svolgimento delle attività di prevenzione, accertamento e repressione dei reati[23].

Oltre a ciò, la normativa in materia di perimetro di sicurezza al cibernetica è connessa anche a quella afferente all'esercizio dei poteri di golden power – ossia, lo strumento normativo che consente al Governo di opporsi all'acquisto di imprese considerate strategiche per l'interesse nazionale, nei settori della difesa, dell'energia, dei trasporti e delle telecomunicazioni e di salvaguardare gli assetti delle imprese operanti in tali settori, anche bloccando determinate delibere aziendali - da parte dell'Esecutivo, atteso che i settori presi in considerazione dal Perimetro di Sicurezza Cibernetica sono i medesimi nei quali può essere esercitato tale potere.

Orbene, dall'analisi di tali provvedimenti legislativi si evince come il legislatore, sia nazionale sia comunitario, abbia inteso attuare interventi di sistema in materia di sicurezza cibernetica, al fine di creare veri e propri meccanismi istituzionali di prevenzione e gestione dei rischi derivanti dall'utilizzo di nuove tecnologie, al fine di tutelare sempre di più l'interesse nazionale e quello dell'Unione Europea.

CamminoDiritto.it
ISSN 2421-7123

9. Conclusioni

Le tematiche affrontate nel presente elaborato, consentono di soffermare l'attenzione sulla Sicurezza Cibernetica e di comprendere come essa non sia una tematica autoreferenziale, ma, invece, rappresenti un argomento connesso a svariati settori d'interesse, tra i più rilevanti dei quali, assurgono la Pubblica Sicurezza e la Sicurezza Nazionale.

La stretta connessione tra la cybersicurezza e i due citati concetti giuridici è, oltretutto, evincibile anche dalla circostanza che taluni reati informatici sono collocati nel codice penale proprio tra i reati contro l'ordine pubblico o la personalità dello Stato (es. art. 270 quinquies co.2 c.p., che prevede l'aggravante della commissione mediante strumenti informatici o telematici di condotte di addestramento ad attività con finalità di terrorismo anche internazionale o l'art. 420 c.p. che sanziona, tra l'altro, gli attentati ai sistemi informatici di pubblica utilità).

Ciò consente, inoltre, di effettuare un'ulteriore, e più profonda riflessione, relativa alle interrelazioni tra diritto e società.

Infatti, il diritto, rappresentando le regole che gli uomini si pongono al fine di disciplinare le relazioni tra i consociati, deve necessariamente prendere in considerazione tutti i fenomeni sociali ed adeguarvisi, altrimenti rischierebbe di diventare, in qualche modo, obsoleto e privo di concreta incisività

Difatti, l'evoluzione tecnologica comporta sovente, non solo modifiche alla legislazione vigente, ma anche al mutamento di taluni concetti giuridici, che devono essere "attagliati" ai mutamenti sociali in atto.

Ebbene, lo sviluppo delle nuove tecnologie ne è una testimonianza. Infatti, dalla loro diffusione in ogni settore della vita umana, ne è derivato l'ampliamento di molti concetti giuridici (non solo quelli presi in considerazione nel presente contributo, ma anche, ad esempio, la privacy) alle attività effettuate mediante strumenti informatici.

Tale considerazione, deve, quindi, indurre gli operatori del diritto ad essere sempre attenti osservatori della realtà sociale, e il legislatore a porre costantemente in atto un'efficace e tempestiva opera di adeguamento della legislazione ai mutamenti della società.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] E. TUCCI, I reati informatici e la Digital Forensics, in AA.VV. L'informatica per il giurista, Santarcangelo di Romagna, 2019, pp.293 e ss.

[2] R. BRIGHI; P. G. CHIARA, La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE , in Federalismi.it – Rivista di diritto pubblico italiano, comparato ed europeo , num. 21/2021, pp. 18 e ss.

[3] G. TROMBETTA, Ordine Pubblico e sicurezza nell'ordinamento italiano, in Democrazia e Sicurezza – Democracy and Security Review, {https/URL}

[4] F. FAMIGLIETTI, La polizia di sicurezza (o "pubblica sicurezza", in F.CARINGELLA;A.IANNUZZI;L.LEVITA, Manuale di diritto di Pubblica Sicurezza, Roma, 2014, p.28.

[5] Così, la voce Ordine Pubblico all'interno dell' Enciclopedia Italiana (1935), a cura di G.PAOLI; G.ZANOBINI.

[6] M.PELLISSERO; M.RIVERDITI, Reati contro la personalità dello Stato e l'ordine pubblico, Torino, 2014, p.225.

[7] V.GREVI, Garanzie costituzionali, ordine pubblico e repressione della delinquenza, in Il Politico , Vol. 41, {https/URL}

[8]Corte Costituzionale, num. 77 del 24 marzo 1987, in {https/URL} (Ultima consultazione 09 febbraio 2022) e Corte Costituzionale num. 278 del 23 giugno 2010 in {https/URL} (Ultima consultazione 09 febbraio 2022).

[9] Al riguardo, giova evidenziare che la Direzione Centrale per la Polizia Criminale ha dichiarato che nel corso dell'anno 2021, infatti, i reati informatici siano stati tra le poche categorie di crimini a registrare un aumento, mentre il numero delle altre tipologie di illeciti penali risultavano in calo.

[10] A.WOLFERS, "National Security" as an Ambiguous Symbol in Political Science Quarterly, Vol. 67, No. 4/1952, pp. 481-502

[11] E.CAMILLI, Sicurezza nazionale tra concetto e strategia in {https/URL}(Ultima consultazione 09 febbraio 2022),p.5.

[12] A.MONTI, Ordine pubblico, sicurezza nazionale e sicurezza cibernetica: una prospettiva di sistema in {https/URL} (ultima consultazione 09 febbraio 2022),p.2.

[13] C.JEAN, cyberwar (voce) in Enciclopedia della Scienza e della Tecnica, 2008.

[14] G.IOVANE, Cyberwarfare e Cyberspace: Aspetti Concettuali, Fasi ed Applicazione allo Scenario Nazionale ed all'ambito Militare, in {https/URL}#160; (ultima consultazione 09 febbraio 2022),p.15.

[16] A.MONTI, Op.cit., pp.5 e 6. [17] Con il termine crittografia di tipo end to end è definita una specifica metodologia di codifica dei messaggi, adoperata da taluni servizi di messagistica istantanea, il cui funzinamento è fondato su algoritmi di crittografia asimettrica e sulla decentralizzazione delle chiavi crittografiche, suscettibile di consentire solo ai soggetti che stanno comunicando la lettura "in chiaro" del testo dei messaggi.

[18] Tribunale Ordinario di Roma, Sezione dei Giudici per le Indagini Preliminari, Ordinanza di Applicazione della Misura della Custodia Cautelare in carcere, emessa nel Procedimento recante {https/URL}://{https/URL}(Ultima consultazione 09 febbraio 2022).

[19] G.D'ALFONSO; F.DONATI;L.FRANCHINA;P.ROSCIOLI;N.VIANELLO, La cyber security nel PNRR: cosa c'è e cosa manca nel piano dell'Italia, in {https/URL}#160;(ultima consultazione 09 febbraio 2022).

[20] L.FRANCHINA; A.LUCARIELLO;L.RUBEO;M.VECCHIATO , Perimetro di sicurezza nazionale e golden power: ecco lo scatto dell'Italia sulla cyber in {https/URL}

CamminoDiritto.it
ISSN 2421-7123

[21]L.FRANCHINA, Perimetro di sicurezza cibernetica e Agenzia dedicata: così la cyber italiana cerca il salto di qualità in {https/URL}#160;(Ultima consultazione 09 febbraio 2022).

[22] R.DE NICOLA; P.PRINETTO, Rivoluzione cyber? Servono tre attori, ecco quali. Scrivono De Nicola e Prinetto, in {https/URL} (Ultima consultazione 09 febbraio 2022).

[23] G.CAMPI, L'impatto della normativa sul perimetro di sicurezza cibernetica sugli acquisti di beni e servizi ICT per la P.A. [L. 18 novembre 2019 n. 133], in {https/URL}#160;(Ultima consultazione 09 febbraio 2022).

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=8123