Premessa

Gli ultimi decenni sono stati caratterizzati da una costante evoluzione tecnologica, che ha avuto ripercussioni considerevoli su ogni aspetto dell'attività umana. È innegabile, infatti, quanto siano divenuti indispensabili per noi tutti gli strumenti tecnologici, il cui utilizzo ha avuto un impatto notevole sui sistemi di comunicazione e sulle relazioni interpersonali. Dispositivi mobili quali *tablet*, *smartphone* e *computer* sono nella piena disponibilità di ciascuno di noi e sono sempre più parte integrante della nostra vita, tanto da potersi parlare addirittura di un "corpo elettronico[1]" che lascia nostre tracce ovunque e che necessita di una tutela esattamente come il "corpo fisico".

La tecnologia informatica si può astrattamente ritenere una tecnologia neutrale, capace, grazie al suo potenziale, di offrire vantaggi e opportunità e al tempo stesso un *humus* fertile per chi la voglia utilizzare per fini criminosi. «Esattamente come un martello può essere adoperato tanto per piantare un chiodo cui appendere un quadro, quanto per fracassare la testa di un uomo, così gli strumenti informatici possono essere impiegati per affermare così come per negare l'esercizio di un diritto»[2]. Questa consapevolezza è stata assunta dal legislatore italiano fin dagli anni '80 del

[1]Sul tema del corpo elettronico e della sua tutela si veda S. RODOTÀ, *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, 2009. Secondo l'Autore, il corpo è inteso come unità funzionale, comprendente anche unità fisicamente collocate in luoghi diversi. L' estensione del corpo e dei suoi diritti oltre i confini della sua unità fisica trova un riscontro evidente quando si parla di "corpo elettronico": "pezzi" di ciascuno di noi sono conservati nelle banche dati dove la nostra identità è scomposta e sezionata, facendoci comparire talvolta consumatori, talvolta elettori, debitori, lavoratori, e così via. Si pone l'esigenza di consentire alla persona di sapere esattamente dove le sue tracce (i suoi "pezzi") sono state lasciate, e di avere accesso diretto alle sue informazioni, ovunque esse si trovino. Da qui il riconoscimento della protezione dei dati personali come diritto autonomo nella Carta dei diritti fondamentali dell'Unione Europea, dove all'art. 8 si afferma che "ogni individuo ha diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica"; sempre S. RODOTÀ nel discorso tenuto nel 2004 quale Presidente dell'Autorità garante per la protezione dei dati personali, ha affermato «Senza una forte tutela del "corpo elettronico", dell´insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo e si rafforzano le spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale: diventa così evidente che la *privacy* è uno strumento necessario per salvaguardare la società della libertà».

[2]F. FAINI – S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, G. Giappichelli Editore,Torino, 2017, p. 239

Novecento, quando ha iniziato ad avvertire l'esigenza di tutelare una particolare categoria di beni giuridici, i c.d. "beni informatici", attraverso la predisposizione di fattispecie penali *ad hoc*. Inizialmente le risposte fornite dal legislatore alle nuove istanze di protezione furono piuttosto frammentate, occasionali e disorganiche[3], costringendo la giurisprudenza a colmare le lacune riconducendo le nuove figure criminose sotto le fattispecie tradizionali. Si sono dovuti attendere degli anni per avere un primo intervento organico con la legge n. 547/1993, sulla spinta di quanto richiesto dal Consiglio d'Europa con la Raccomandazione del 1989.

Le riforme che negli ultimi anni si sono rese necessarie per contrastare le problematiche sorte dall'avvento dell'era del digitale, hanno toccato sia profili sostanziali, sia profili procedurali del diritto penale. Da un lato, infatti, l'ordinamento ha reagito al fenomeno della criminalità informatica attraverso l'introduzione di nuove fattispecie penali; dall'altro lato, gli strumenti informatici sono apparsi fin da subito possibili contenitori di informazioni, utili ai fini probatori. La c.d. prova digitale si annida sempre più all'interno dell'accertamento di qualsiasi tipologia di reato, compresi quei reati comuni, totalmente privi di una dimensione tecnologica (si pensi, ad esempio, ad un omicidio). Si è resa necessaria l'introduzione di nuove forme di indagini informatiche, che si pongono spesso in frizione col rispetto delle garanzie individuali che la Costituzione *in primis* riconosce. Il nodo problematico sta quindi nel cercare di bilanciare due opposte esigenze: l'accertamento del fatto di reato e la tutela dei diritti fondamentali degli individui coinvolti in tale accertamento. Il rischio che si deve cercare di evitare in modo particolare è una ingerenza sconsiderata nel diritto alla *privacy* e alla riservatezza delle persone[4]. Nodo che si fa ancora più

[3]P. SCOGNAMIGLIO, *Criminalità informatica. Commento organico alla Legge 18 marzo 2008, n. 48*, Simone, Napoli, 2008, p. 5 ss.

[4]Per quanto riguarda la definizione di "riservatezza", la dottrina non è unanime. C'è chi propone che si debba parlare genericamente di "*privacy*", chi invece propende verso l'introduzione del termine "privatezza", chi ancora preferisce parlare di "rispetto della vita privata" o più semplicemente di "vita privata". F. MANTOVANI, *Diritto penale. Delitti contro la persona*,

problematico laddove si prenda consapevolezza del fatto che la prova digitale (*digital evidence*) è caratterizzata da una elevata volatilità e facile alterabilità da parte di chiunque entri in contatto con il dato informatico in essa raccolto, facendo sorgere delicate questioni di tipo processuale, con riferimento alle corrette modalità di acquisizione, conservazione e presentazione della prova in giudizio.

Sulla base di queste seppur brevi considerazioni, si capisce quanto importante e delicato sia il rapporto che intercorre tra il mondo della tecnologia dell'informazione e il mondo del diritto, che ha portato in questi ultimi decenni il legislatore ad occuparsi della materia, sia a livello nazionale che internazionale. Il punto di arrivo di questo percorso normativo è rappresentato dalla Convenzione di Budapest sulla cybercriminalità del 2001, ratificata in Italia con la legge n.48/2008.

Cedam, Padova, 2016, p. 590; F. MUCCIARELLI, *Informatica e tutela penale della riservatezza*, in L. PICOTTI, *Il diritto penale dell'informatica nell'epoca di internet*, Cedam, Padova, 2004, p. 185. Secondo MANTOVANI è preferibile si debba parlare di "riservatezza" perché: "vita privata" per la sua omnicomprensività abbraccia beni distinti che devono essere terminologicamente differenziati; inoltre la "vita privata" è rappresentata da un insieme di fatti e non di valori; quindi, oggetto giuridico non può essere la "vita privata" ma la "privatezza della vita", o per meglio dire, la "riservatezza". Per "riservatezza" si intende l'interesse a che nessuno conosca e quindi alla esclusività di conoscenza.

CAPITOLO I. IL QUADRO NORMATIVO EUROPEO SULLA CRIMINALITÀ INFORMATICA

1. Gli interventi internazionali per contrastare la criminalità informatica

La Convenzione chiude un percorso normativo internazionale[5], iniziato con l'elaborazione ad opera dei *working group* in sede OCSE di una lista comune di reati informatici nel 1983, prospettandosi già allora l'idea di una possibile applicazione e armonizzazione a livello internazionale di leggi penali al fine di contrastare il fenomeno della criminalità informatica. L'opera di armonizzazione è proseguita con la redazione di un rapporto da parte di un gruppo di esperti, riuniti dal Comitato per la Politica dell'Informazione, dell'Informatica e delle Comunicazioni dell'OCSE; gli esperti, tra il 1984 e il 1985 analizzarono i principali orientamenti normativi degli Stati membri dell'organizzazione nel settore della criminalità informatica e le soluzioni già concretamente adottate. Nel 1986 l'OCSE ha pubblicato la relazione *Computer-related crime: Analysis of Legal Policy* con lo scopo di offrire proposte di riforma per la creazione di un elenco di quegli abusi informatici ritenuti essenziali, che necessariamente sarebbero dovuti essere puniti dal legislatore penale nazionale. Nel 1992 sono state pubblicate per la prima volta le *Linee guida sulla sicurezza dei sistemi e delle reti d'informazione*[6] dell'OCSE. Tutto il settore delle tecnologie dell'informazione ha provocato notevoli

[5]Si veda G. CORASANITI, G. CORRIAS LUCENTE, *Cybyercrime, responsabilità degli enti, prova digitale, Commento alla Legge 18 marzo 2008, n.48*, Cedam, Padova,2009, p. 2 e ss; L. LUPÁRIA- G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Giuffrè Editore, Milano, 2007, p. 211.

[6]*https://www.oecd.org/sti/ieconomy/15582268.pdf*

cambiamenti nelle società, offrendo indiscutibili vantaggi ed opportunità, ma richiedendo altresì una maggiore attenzione alla sicurezza da parte di governi, imprese, istituzioni e singoli utenti, che possiedono, gestiscono, utilizzano quotidianamente i sistemi e le reti informatiche. *Internet* ha assunto un ruolo centrale per lo svolgimento delle attività d'impresa, per la fornitura di servizi ai cittadini, per la comunicazione e lo scambio di informazioni tra le persone. I sistemi informatici e le reti d'informazione sono sempre più interconnessi, e ciò comporta un aumento esponenziale di minacce e di vulnerabilità, richiedendo un intervento a tutela della sicurezza nella comunicazione. Sulla base di queste considerazioni, l'OCSE già nel 1992 ha avvertito l'esigenza di sviluppare una "cultura della sicurezza" nella nuova società dell'informazione, attraverso l'adozione delle linee guida rivolte a tutte le parti interessate.

In sede G8,l'*HighTech Sub-working group* ha elaborato nel 1997 una serie di principi operativi comuni oltre ad un programma di azione; da questo progetto, l'anno successivo sono nati dei gruppi di contatto a supporto delle investigazioni nei casi di *computer crimes,* il c.d. *24-hour, seven day network* (ripreso, come vedremo, dalla Convenzione di Budapest all'art.35). Queste iniziative hanno voluto assicurare una cooperazione internazionale effettiva nell'ambito delle investigazioni informatiche, predisponendo gli strumenti giuridici e tecnici, utili agli investigatori. Si può ritenere che, in un certo senso, tali previsioni abbiano contribuito a costituire la base della Convenzione di Budapest, tanto da essere richiamate nel preambolo della Convenzione stessa.

Nel G8 si è proceduto ad individuare una categoria di "minacce informatiche", che adesso trova un riconoscimento ufficiale proprio all'interno della Convenzione; in particolare si distinguono i reati commessi *contro* e i reati commessi *per mezzo di computer*, la cui commissione risulta facilitata proprio dall'utilizzo del dispositivo informatico. Dal punto di vista metodologico, i principi di fondo fatti propri dal G8 richiedono in linea

generale che, ogni qualvolta si debba intervenire per contrastare il *cybercrime*, occorra agire rapidamente e con grande professionalità, salvaguardando gli elementi di prova, che si trovano in un ambiente in cui possono facilmente essere perduti o distrutti. Altro elemento critico da dover affrontare riguarda il carattere transnazionale della criminalità informatica, per cui si sono individuati strumenti investigativi utili per fronteggiare al meglio questo particolare aspetto, richiedendo agli Stati di intervenire attuando meccanismi di cooperazione internazionale. Dal punto di vista organizzativo, il G8 ha istituito a livello nazionale unità speciali di polizia informatica ed in linea generale ha cercato di implementare gli strumenti di contrasto ai *computer crimes*.

2. La raccomandazione n. R(89) 9 sulla criminalità in relazione all'elaboratore

I problemi derivanti dal fenomeno della criminalità informatica hanno catturato l'attenzione della dottrina penalistica a partire dagli anni '80 del secolo scorso, quando si iniziarono a verificare le prime pratiche illecite collegate all'uso della tecnologia. In Italia, come altrove, venivano commessi sempre più crimini connessi con l'uso dell'elaboratore elettronico, che avevano ad oggetto in particolare i sistemi bancari. Lo scopo era quello di alterare il funzionamento dei sistemi di trasferimento elettronico di fondi, e di accreditare a sé stessi ingenti somme di denaro. Sempre nello stesso periodo, poi, iniziarono a diffondersi i c.d. *hackers*, che commettevano (e tutt'ora commettono) i reati non tanto per fini di lucro, ma per il semplice gusto di farlo, di dimostrare la propria abilità nell'aggirare i sistemi di protezione dei dispositivi informatici[7].

[7]F. FAINI – S. PIETROPAOLI, op. cit., p.240; E. GIANNANTONIO, *L'oggetto giuridico dei reati informatici*, Cass. pen., fasc.7-8, 2001, pag. 2029. Si trattava di reati ai quali erano stati dati nomi piuttosto particolari, come *data diddling*, *logicbombing*, *piggy-backing*, *trojanhorsing*,

Per cercare di fornire una risposta omogenea ed uniforme alla questione, è intervenuto il Consiglio d'Europa, mediante l'approvazione della Raccomandazione n. R(89) 9 sulla criminalità in relazione con l'elaboratore, redatta dal Comitato Direttore per i Problemi Criminali (CDPC). Questo documento conteneva due liste di reati informatici; una lista "minima" e una "facoltativa". Nella prima vennero inserite quelle condotte criminose che, secondo il Consiglio, gli Stati membri avrebbero dovuto urgentemente riconoscere ed incriminare (si trattava dei reati di frode informatica, falso informatico, danneggiamento dei dati e dei programmi informatici, accesso abusivo, riproduzione non autorizzata di software, sabotaggio informatico). Nella seconda vennero elencate invece quelle condotte non altrettanto offensive, ma bisognose comunque di un intervento del legislatore nazionale (quali l'alterazione non autorizzata di dati o programmi senza loro danneggiamento, la divulgazione di informazioni legate al segreto industriale o commerciale, l'utilizzazione non autorizzata di un elaboratore elettronico o di un programma informatico protetto).

Segue: brevi cenni sulla legge 547/1993

Alla luce di quanto richiesto dall'Unione Europea, il legislatore italiano è intervenuto con la legge 23 dicembre del 1993, n. 547, recante "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica". Il problema che è si è

salami technique. Era chiaro a tutti che queste condotte fossero illecite e si avvicinassero molto agli estremi della truffa, anche se poi di fatto mancavano artifizi o raggiri necessari per indurre in errore una persona, quali elementi necessari del dolo per la configurabilità del reato. Infatti, in tutti questi casi, si cercava di incidere sul funzionamento di una macchina, senza prendere minimamente in considerazione l'uomo e la sua libertà di autodeterminarsi.

dovuto affrontare nel dare attuazione alla Raccomandazione, è stato se considerare necessaria l'introduzione di una legge speciale *ad hoc* o se limitarsi a modificare il codice penale, riconducendo i nuovi reati alle figure già previste e disciplinate dal codice. La scelta è ricaduta sulla seconda soluzione, riflettendo la consapevolezza che non si stessero introducendo fattispecie volte a tutelare beni giuridici nuovi, ma solo tutele contro nuove forme di aggressione ai beni già considerati dall'ordinamento come meritevoli di protezione[8].

La legge ha introdotto 14 norme penali che sono state inserite nel libro II del codice penale, intervenendo principalmente in quattro settori[9]: quello delle "frodi informatiche" che hanno la peculiarità di essere perpetrate col mezzo informatico (senza indurre nessuno in errore); quello delle "condotte di falsificazione" estese ai documenti predisposti da un sistema informatico e telematico, perciò diversi dai documenti tradizionali; quello delle "aggressioni all'integrità dei dati e dei sistemi informatici" e quello delle "aggressioni alla riservatezza dei dati e delle comunicazioni informatiche". Rispetto ai precedenti interventi del nostro legislatore in questa materia, caratterizzati per la loro frammentarietà e settorialità, sicuramente questa novella risulta essere la più organica; ma il processo riformatore si è tutt'altro che fermato. La legge n. 547 può essere letta allora come un punto di svolta nell'evoluzione del diritto penale dell'informatica, segnando il passaggio dalla fase dei *computer crimes* classici alla fase più moderna del *cybercrime*[10].

---

[8]P. SCOGNAMIGLIO, op. cit., p. 8. Secondo l'Autore la creazione di una ennesima legge speciale avrebbe potuto confinare la materia della criminalità informatica in un settore non centrale dell'ordinamento. Per questo si è cercato di estendere le previsioni codicistiche già esistenti (ad esempio il danneggiamento o la truffa) alle nuove condotte criminose e si sono introdotte nuove figure, come frode informatica, danneggiamento di sistemi informatici, accesso abusivo a un sistema informatico.

[9] D. D'AGOSTINI, *Diritto penale dell'informatica, dai computer crimes alla digital forensics*, Experta, Forlì, 2007, p.10

[10] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), op.cit., p. 28. Come sottolinea l'Autore, è proprio a partire dagli anni '90 che si diffonde in maniera sempre più dilagante l'utilizzo di *Internet*, quale rete informatica globale che consente l'accesso e la comunicazione da parte di chiunque,

3. La Raccomandazione n. R(95) 13 relativa ai problemi di procedura penale legati alla tecnologia dell'informazione

La Raccomandazione n. R (95) 13 dell'11.09.1995 *relativa ai problemi di procedura penale legati alla tecnologia dell'informazione* chiede ai governi degli Stati membri di ispirarsi, nel momento in cui modificano le legislazioni e procedure interne, ai principi generali annessi alla Raccomandazione. In virtù del necessario coordinamento e adattamento richiesto, gli Stati avrebbero dovuto applicare a livello normativo la «distinzione operata dal diritto tra la perquisizione dei sistemi informatici, il sequestro dei dati raccolti e l'intercettazione di dati in corso di trasmissione» (art. 1), consentendo in sostanza alle autorità nazionali di effettuare perquisizioni dei sistemi informatici e sequestri dei dati in essi racchiusi in condizioni analoghe a quanto disposto dalla normativa tradizionale. In particolare, il responsabile del sistema dovrebbe essere informato che il sistema è oggetto di perquisizione e sequestro, oltre che sulla natura dei dati sequestrati. Inoltre, ogni volta che si verifica una equivalenza funzionale tra il dato informatico e il documento tradizionale, le perquisizioni e i sequestri informatici dovrebbero avvenire sulla base delle disposizioni riferite ai documenti. I dati raccolti attraverso le intercettazioni dovrebbero essere salvaguardati in maniera appropriata; si chiede alle leggi di procedura penale di rendere in concreto possibile l'intercettazione dei dati nell'ambito di inchieste su reati gravi contro la riservatezza, l'integrità e l'accesso a sistemi di telecomunicazioni o informatici[11].

L'art. 13 della Raccomandazione manifesta l'esigenza di garantire la genuinità della prova elettronica. Si chiede agli Stati di «raccogliere, di

provocando una trasformazione evidente delle forme di criminalità nonché l'estensione dei comportamenti illeciti anche in rete.

[11]G. CORASANITI, G. CORRIAS LUCENTE, op. cit., p. 26.

salvaguardare e di esibire prove elettroniche in modo da garantire al meglio il carattere inconfutabile e l'integrità di esse»[12].Tale interesse comune sorge da una acquisita triplice consapevolezza: i *computer* possono talvolta costituire vere e proprie fonti di prova. Come fonti di prova, però, i *computer* sono unici, così come unici sono gli elementi di prova che da essi scaturiscono[13]. Sul tema tratteremo in maniera più approfondita successivamente; quello che in questo contesto rileva è che con tale raccomandazione si è chiesto agli Stati di predisporre strumenti idonei a garantire la conservazione e la non alterabilità del dato digitale.

Quanto affermato nella Raccomandazione costituisce la struttura essenziale di quello che può essere identificato come il più ambizioso progetto legislativo nato per contrastare il fenomeno del *cybercrime*. Si tratta della Convenzione di Budapest del Consiglio d'Europa, approvata nel 2001 e entrata in vigore nel 2004.

4. La Convenzione del Consiglio d'Europa sul *Cybercrime* (Budapest, 23 novembre 2001)

4.1. Lavori preparatori alla Convenzione di Budapest[14]

Il Comitato Direttore per i Problemi Criminali[15] (CDPC), preoccupato della crescita esponenziale della tecnologia e delle nuove minacce alla sicurezza, alla riservatezza e al patrimonio, in linea con quanto

[12]L'art. 13 della Raccomandazione prosegue stabilendo che «A tale fine, procedure e metodi tecnici per il trattamento delle prove elettroniche dovrebbero essere sviluppati preventivamente in modo da assicurarne la compatibilità tra Stati. Le disposizioni del diritto di procedura penale concernenti le prove e riferibili a documenti tradizionali dovrebbero ugualmente applicarsi ai dati immagazzinati in un sistema informatico.»

[13]F. M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in Cass. Pen., fasc. 2, 2012, p. 0696B

[14]C. SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, Giuffrè Editore, Milano, 2010, p. 587 ss.

[15] Si tratta dell'organo del Consiglio d'Europa incaricato del disegno della politica criminale dell'Unione Europea.

intrapreso a partire dagli anni ’80 con la Raccomandazione n. R(89) 9 *sulla criminalità in relazione con l’elaboratore* e la Raccomandazione n. R(95) 13 sui *problemi di procedura penale collegati alla tecnologia dell’informazione*, nel 1996 decise di istituire un Comitato di esperti sul problema della criminalità informatica. Il lavoro svolto dagli esperti si ispirò ad un principio fondamentale: «la dipendenza sociale, economica e culturale dall’informazione contenuta nelle reti di comunicazione ed in particolar modo da Internet impone la tutela di beni giuridici fondamentali che entrano in gioco[16]».

A seguito di questa decisione, nel 1997 venne creato il “Comitato di esperti sulla criminalità nello spazio cibernetico” il cui compito è stato quello di redigere uno schema di convenzione. Il Comitato ha iniziato a svolgere il suo incarico nel 1997, portandolo a termine tre anni dopo, nel 2000, con la presentazione di uno schema di convenzione, poi divenuta la Convenzione di Budapest.

La versione definitiva di questo schema è stata presentata al Comitato per l’approvazione. Una volta approvata, la Convenzione è stata trasmessa al Comitato dei Ministri, che l’ha adottata. Il 23 novembre del 2001, a Budapest, il Comitato stesso ha deciso di aprire la Convenzione alla sottoscrizione da parte degli Stati membri.

La Convenzione è entrata ufficialmente in vigore il 1° luglio del 2004, una volta intervenute le ratifiche richieste dal Trattato stesso[17]. Ad oggi le adesioni al Trattato risultano pari a 60[18].

---

[16]O. MORALES GARCÍA, *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d’Europa sul Cyber-crime*, in L. PICOTTI (a cura di), op. cit., p. 128

[17]L’art. 36 della Convenzione, intitolato “Firma ed entrata in vigore”, recita così:
«La presente Convenzione è aperta alla firma degli Stati membri del Consiglio d'Europa e degli Stati non membri che hanno partecipato alla sua elaborazione.
La presente Convenzione è soggetta a ratifica, accettazione o approvazione. Gli strumenti di ratifica, accettazione o approvazione sono depositati presso il Segretario generale del Consiglio d'Europa.
La presente Convenzione entra in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dopo la data in cui cinque Stati, di cui almeno tre Stati membri del Consiglio

La portata e la struttura della Convenzione riflettono le mancate iniziative a livello nazionale e internazionale in questa materia, tanto da indurre gli esperti ad adottare decisioni fondamentali relative alla Convenzione stessa. Innanzitutto, si è preferito intervenire attraverso una Convenzione e non una semplice Raccomandazione (come già era stato fatto in passato), per consentire un'effettiva opera di armonizzazione della normativa penale dei vari Stati sia dal punto di vista sostanziale che procedurale, oltre che sul piano della cooperazione e collaborazione internazionale. In secondo luogo, il Comitato ha deciso di rendere il Trattato aperto alla firma non solo degli Stati membri del Consiglio, ma anche di quei Paesi extracomunitari che hanno partecipato alla elaborazione del suo contenuto[19].

4.2. Cenni generali sulla struttura della Convenzione

La Convenzione del Consiglio d'Europa sulla criminalità informatica rappresenta il primo accordo internazionale che si occupa di questa materia, sulla scia di quanto delineato già con la precedente Raccomandazione n. R(95) 13 del 1995. Con questo Trattato, il Consiglio d'Europa ha cercato di fornire una soluzione globale ed uniforme al fenomeno internazionale della criminalità informatica, che rischia di rendere le società moderne sempre

d'Europa, abbiano espresso il loro consenso ad aderire alla Convenzione conformemente alle disposizioni dei paragrafi 1 e 2.
Per gli Stati firmatari che esprimono successivamente il loro consenso ad aderire alla Convenzione, questa entra in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dopo la data in cui tali Stati esprimono il loro consenso a essere vincolati dalla Convenzione conformemente alle disposizioni dei paragrafi 1 e 2.»
La Convenzione, quindi, è entrata in vigore quando sono intervenute le 5 ratifiche richieste, 3 delle quali provenienti dai Paesi appartenenti al Consiglio d'Europa.
Tra i Paesi firmatari, figurano anche quattro Paesi extracomunitari, che pur non facenti parte del Consiglio d'Europa, hanno partecipato alla elaborazione della Convenzione (si tratta di Stati Uniti, Canada, Giappone, Sud Africa).

[18]In base a quanto risulta dalla *webpage* ufficiale del Consiglio d'Europa *www.coe.int,* consultata nel Luglio 2018.

[19], O. MORALES GARCÍA, in L. PICOTTI (a cura di),op. cit., p. 129 ss.