CRIO WORKSHOP
CENTRE OF RESEARCH ON INTERNATIONAL ORGANIZATIONS

CRIO PAPERS

N°.59

MARILENA ARENA

LA CONVENZIONE DI BUDAPEST DEL CONSIGLIO D'EUROPA SULLA REPRESSIONE DELLA CRIMINALITA' INFORMATICA

CRIO Papers A Student-Led Interdisciplinary Paper Series
ISSN: 2037-6006
The School of Laws
University of Catania
Villa Cerami I – 95124 Catania Italy

1. Considerazioni introduttive

La Convenzione del Consiglio d'Europa, nota come Convenzione di Budapest, è uno strumento di primaria importanza, il maggior sforzo finora effettuato nella lotta al Cybercrime.

Essa svolge un ruolo cruciale nella lotta contro la criminalità informatica; stabilisce standard di diritto penale basati su principi all'avanguardia e norme procedurali inerenti l'archiviazione provvisoria dei dati da utilizzare potenzialmente come prova nel perseguire atti criminali.

Alexander Seger, Capo della Divisione della Criminalità informatica del Consiglio d'Europa, ha sottolineato che la Convenzione di Budapest rimane, ad oggi, lo strumento internazionale più efficiente:

"*La Convenzione di Budapest è sinonimo di una visione di un Internet libero, dove le informazioni possono fluire liberamente, essere consultate e condivise, dove le restrizioni sono definite in modo restrittivo per contrastare l'uso improprio e dove vengono indagati e perseguiti solo reati specifici, fatte salve le necessarie garanzie"*[1].

In termini generali, la Convenzione di Budapest prevede:

- la criminalizzazione di condotte criminose: dall'accesso illegale all'attentato all'integrità di un sistema, dalla frode informatica alla pornografia infantile;
- strumenti di diritto processuale, al fine di svolgere indagini per la lotta alla criminalità informatica e per la ricerca di prove elettroniche sicure in relazione a qualsiasi crimine;
- una cooperazione internazionale efficiente.

[1] Per ulteriori precisazioni consultare il sito web del Consiglio d'Europa all'indirizzo www.coe.int/en/web/cybercrime.

La convenzione presenta carattere innovativo e flessibile.

Innovativo poiché ha ad oggetto il mondo digitale, come si evince dai continui riferimenti ai sistemi informatici, ai dati e alla rete.

In merito alla flessibilità, bisogna attenzionare la natura di disciplina 'quadro' della Convenzione[2]: le parti negoziali hanno disciplinato gli aspetti sui quali sono riuscite a trovare un accordo. Altrettanto importanti sono quelle problematiche, discusse dalle parti negoziali, sulle quali non è stata raggiunta un'intesa. Nulla esclude che un accordo possa avvenire anche in futuro. Ad esempio, durante i lavori preparatori della Convenzione, non è stato possibile raggiungere un accordo tra le parti relativamente al reato di diffusione in rete di propaganda razzista. Sebbene vi sia stato un significativo sostegno a favore dell'inclusione di questo crimine, notando la complessità del problema si decise di rinviare la questione al Comitato Europeo per i problemi della criminalità (CDPC), che ebbe il compito di elaborare un protocollo addizionale: "*Il protocollo aggiuntivo alla convenzione sulla criminalità informatica, relativo alla criminalizzazione di atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici*", firmato a Strasburgo nel 2003[3].

Grazie alla struttura flessibile della Convenzione, è stato possibile estendere il suo raggio operativo anche a tali reati, fornendo alle parti la possibilità di utilizzare mezzi e vie di cooperazione in essa stabilite.

Con l'avvento del 'cloud computing'[4]è in atto dal 2017 la preparazione di un secondo protocollo aggiuntivo contenente misure destinate esclusivamente a indagini penali specifiche. I lavori preparatori hanno portato alla redazione di cinque testi provvisori che, qualora adottati nella versione finale del secondo Protocollo, sarebbero vincolanti

---

[2] G. Ilarda e G. Marullo, *Cybercrime: Conferenza Internazionale. La convenzione del consiglio d'Europa sulla criminalità informatica,* Milano 2004, p. 43.

[3] Treaty NO. 189, "*Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems"*. Indirizzo web www.coe.int/it/web/conventions/full-list

[4] Dal punto di vista tecnologico, secondo la definizione del NIST (National Institute for Standards and Technology), il Cloud Computing è un insieme di servizi ICT accessibili on-demand e in modalità self-service tramite tecnologie Internet, basati su risorse condivise, caratterizzati da rapida scalabilità e dalla misurabilità puntuale dei livelli di performance, in modo da poter essere pagati in base al consumo.

solo per le parti della Convenzione di Budapest che vi hanno ufficialmente acconsentito.

La disconnessione tra la giurisdizione territoriale degli Stati e il modo in cui i dati si spostano e sono conservati attraverso i confini nazionali, pone sfide significative per le forze dell'ordine. Il fine è quello di affrontare le sfide della giustizia penale nel cyberspazio, tramite una cooperazione più efficace in materia di criminalità informatica, nonché garantire un internet libero, in cui i governi nazionali abbiano, come compito principale, quello di proteggere le loro persone e i loro diritti.

Caratteristica che contraddistingue la Convenzione è la trasparenza del processo di redazione. Il Comitato ha deciso di pubblicare i risultati dei lavori preparatori sul sito web del Consiglio d'Europa; riteneva che la pubblicazione delle prime bozze fosse necessaria a favorire l'apertura del processo negoziale per fornire agli Stati informazioni per rafforzare il dibattito in ambito nazionale.

Nonostante qualsiasi Paese possa servirsi della Convenzione come linea guida per la propria legislazione nazionale, è corretto affermare che esserne Parte comporta una serie di vantaggi.

Essa rappresenta la base giuridica per la cooperazione internazionale ed è in continua fase evolutiva grazie alla possibilità delle Parti di aggiungere note di orientamento e protocolli. Esserne parte significa anche appartenere alla rete di professionisti che è stata istituita dal presente Trattato per il miglioramento dell'efficienza delle indagini a livello sovranazionale (rete 24 ore su 24, 7 giorni su 7), nonché migliorare la cooperazione con il settore privato.

La peculiarità della Convenzione deriva dalla composizione del gruppo degli Stati firmatari: non solo Stati membri del Consiglio d'Europa. Il coinvolgimento di Stati non appartenenti al COE dimostra che è possibile ottenere risultati comuni tra Paesi provenienti da tradizioni giuridiche diverse. Questo Trattato deve essere visto come uno sforzo veramente "internazionale", non esclusivamente europeo, che può accogliere concetti giuridici non europei e, in quanto tale, rendere più semplice l'adesione successiva di altri Stati.

Gli Stati che hanno firmato la Convenzione sono 68, di cui 65 hanno proceduto alla ratifica. Di questi, gli appartenenti al consiglio d'Europa sono 47: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgio, Bosnia e Erzegovina, Bulgaria, Cipro, Croazia, Danimarca, Estonia, Federazione Russa, Finlandia, Francia, Georgia, Germania, Gran Bretagna, Grecia, Irlanda, Islanda, Italia, Lettonia, Liechtenstein, Lituania, Lussemburgo, Malta, Monaco, Montenegro, Nord Macedonia, Norvegia, Paesi Bassi, Polonia, Portogallo, Repubblica Ceca, Repubblica di Moldavia, Repubblica Slovacca, Romania, San Marino, Serbia, Slovenia, Spagna, Svezia, Svizzera, Turchia, Ucraina, Ungheria. I paesi extraeuropei sono: Argentina, Australia, Benin, Brasile, Burkina Faso, Canada, Capo Verde, Cile, Colombia, Costa Rica, Filippine, Ghana, Giappone, Guatemala, Israele, Marocco, Mauritius, Messico, Niger, Nigeria, Nuova Zelanda, Panama, Paraguay, Perù, Repubblica Dominicana, Senegal, Sri Lanka, Stati-Uniti d'America, Sud Africa, Tonga, Tunisia[5].

L'impatto della Convenzione di Budapest nelle legislazioni nazionali non è limitato, esclusivamente, agli stati firmatari. Ciò trova conferma in un sondaggio sullo stato globale della legislazione sulla criminalità informatica, concluso nel febbraio 2020, i cui risultati vengono esposti qui di seguito:

- circa 177 Stati (92%) in tutto il mondo hanno posto in essere delle riforme o sono stati in procinto di farlo;
- non solo le Parti hanno attinto alla Convenzione di Budapest per la riforma della loro legislazione, ma circa 153 (79%) membri delle Nazioni Unite l'hanno utilizzata come linea guida o come fonte per le loro riforme;
- circa 106 Stati (55%) sembrano aver adottato disposizioni nazionali specifiche corrispondenti in linea di massima agli articoli di diritto penale sostanziale della Convenzione di Budapest;

[5] Sito web del Consiglio d'Europa, www.coe.int/it/web/conventions/full-list

- circa 82 Stati (42%) disponevano in gran parte di poteri procedurali specifici, mentre molti Stati hanno fatto affidamento su disposizioni procedurali generali per indagare sulla criminalità informatica e salvaguardare le prove elettroniche. Riformare il diritto processuale e promulgare poteri procedurali specifici per proteggere le prove elettroniche da utilizzare nei procedimenti penali (corrispondenti agli articoli da 16 a 21della Convenzione di Budapest e soggetta alle garanzie di cui all'articolo 15) è impresa più complessa.[6]

2. Finalità

Prima di procedere all'analisi delle disposizioni introdotte, è necessario individuare gli obiettivi che hanno spinto il Consiglio d'Europa alla redazione della Convenzione di Budapest.

Autorevole dottrina afferma che:

«*L'obiettivo primario della Convenzione sulla criminalità informatica risiede nell'esigenza di introdurre un minimum target di tutela dei beni giuridici offesi dai cybercrimes ed un livello minimo essenziale comune di strategie di contrasto a tali illeciti, soprattutto in ragione della loro natura tendenzialmente transnazionale, che comporta chiaramente la necessità dell'armonizzazione della relativa normativa di contrasto nell'ambito dei vari ordinamenti*»[7].

I temi principali sono la prevenzione di atti criminali e il coordinamento delle forze dell'ordine internazionali. Viene affrontata, inoltre, la tematica relativa all'incidenza delle disposizioni convenzionali sui "diritti umani fondamentali".

[6] Council of Europe, *The Budapest Convention on Cybercrime: benefits and impact in practice,* Strasbourg, 13 July 2020
https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional

[7] Resta, Cybercrime e cooperazione internazionale nell'ultima legge della legislatura, in *Corriere del Merito,* Torino, 2008.

Dal preambolo della Convenzione, si evince come la questione prioritaria, ben chiara e consolidata nelle intenzioni del Consiglio d'Europa, è quella di cercare una '*politica comune*'[8], finalizzata a proteggere le società dai cyber crimini. I mezzi predisposti a tal fine saranno l'armonizzazione delle procedure nazionali e il potenziamento dell'assistenza giudiziaria in questi settori.

La nuova normativa è importante perché istituzionalizza a livello giuridico una classificazione globalmente valida dei possibili reati informatici e predispone una definizione inerente ai differenti dispositivi elettronici.

I fini perseguiti dalla Convenzione sono molteplici.

In primo luogo è un deterrente per azioni dirette contro la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati informatici, così come per l'uso improprio di questi sistemi. L'attività di dissuasione consiste nella criminalizzazione di questi comportamenti e nell'adozione di poteri sufficienti a combattere realmente questi reati, facilitando la loro individuazione, investigazione e l'esercizio dell'azione penale a livello nazionale ed internazionale, prevedendo accordi per una cooperazione internazionale più veloce e affidabile[9].

In secondo luogo la Convenzione, mediante il rinvio alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (firmata a Roma il 4 novembre 1950), al Patto internazionale sui diritti civili e politici (adottato a New York il 16 dicembre 1966 ed entrato in vigore il 23 marzo 1976) e a ogni altro strumento internazionale applicabile, ha uno scopo ulteriore: la necessità di cercare un soddisfacente livello di bilanciamento tra misure statali restrittive dell'accesso ad Internet, perché repressive di condotte caratterizzate da un qualche disvalore, da un lato, e il rispetto dei diritti fondamentali, dall'altro.

Il Trattato in esame mira, inoltre, a fornire un quadro normativo comune alla luce del quale i Paesi membri possano procedere all'armonizzazione del diritto penale nazionale e dei codici di rito in materia di reati commessi via Internet.

[8] Convenzione di Budapest sulla criminalità informatica, Preambolo, https://rm.coe.int/1680081561
[9] Convenzione di Budapest, cit. p. 50

3. La Convenzione come modello di armonizzazione

"*L'armonizzazione del diritto internazionale è indispensabile laddove un controllo nazionale non è più possibile ...: dove c'è antagonismo tra responsabili che operano a livello globale e sistemi di diritto penale nazionale…In quest'area globale del 'cyberspazio' sono necessarie almeno un minimo di regole comuni… D'altra parte, non c'è urgenza di armonizzare le regole del diritto processuale penale...altamente correlate alle differenze nazionali negli sviluppi culturali e storici …"*[10].

L'armonizzazione mira alla creazione di una regolamentazione efficace di un fenomeno globale, nel rispetto delle differenze nazionali. Essa è indispensabile laddove un controllo statale non è possibile a causa della presenza di attori globali[11].
Il cybercrime è, è il crimine internazionale per eccellenza anche quando è commesso in ambito locale. È prioritario che le normative degli Stati siano tali da prevedere la perseguibilità dei reati allo stesso modo in ogni Paese, poiché '*legislazioni armonizzate'* facilitano meccanismi cooperativi tra le forze dell'ordine, sia nel contesto europeo che in quello internazionale[12].
L'armonizzazione delle procedure dei Paesi in ambito di criminalità informatica, in un contesto variegato di legislazioni, entra in conflitto con le differenze culturali e storiche, nonché con le diverse tradizioni giuridiche.
Sebbene essa è auspicabile, ogni nazione ha il proprio modo di concepire la criminalità, l'adeguatezza della punizione, la proporzionalità delle pene e dei diritti riconosciuti all'imputato.

[10] Miriam F. Miquelon- Weismann, op. cit.p.27.
[11] Termine adoperato nell'Unione Europea con cui si indica il processo di progressivo ravvicinamento delle legislazioni degli Stati membri, al fine di eliminare ogni ostacolo tecnico, amministrativo o normativo alle relazioni dell'Unione.
[12]G. Ilarda e G. Marullo, op. cit. p. 45.

Nello scenario conseguente l'incessante sviluppo della criminalità informatica, il processo di armonizzazione tra i Paesi è l'obiettivo principale.

L'essenzialità di questo processo trova la sua ragion d'essere in due considerazioni di fondo. La prima è evitare la creazione di 'rifugi sicuri' o eliminarli. Si tratta di problemi legati al principio di 'doppia incriminazione'[13]: se la condotta non è criminalizzata in un Paese specifico, le persone in quel Paese possono agire, senza essere incriminate, nel commettere reati che interessino altre giurisdizioni. Sorgeranno problematiche sia in ambito di raccolta delle prove informatiche che in materia di estradizione, dato che le condotte illecite sarebbero commesse in luoghi dove il disvalore del fatto non è percepito come integrante una fattispecie di reato. La seconda considerazione individua l'armonizzazione come strumento fondamentale per una cooperazione efficace tra le forze dell'ordine e autorità giudiziarie degli Stati coinvolti nel perseguimento dei crimini.

I danni, effettivi o potenziali, causati da tali reati informatici non devono essere sottovalutati.

Entrare in un sistema informatico e introdurre un virus può facilmente portare alla distruzione di dati o interi sistemi in tutto il mondo a causa di reti interconnesse.

Occorre una precisazione: 'armonizzato' non vuol dire 'identico'[14].

Ciò che conta è la complementarietà delle discipline, ossia gli strumenti utilizzati da ogni Stato devono avere come obiettivo il perseguimento del fenomeno criminale, sconfiggendolo, seppur tenendo conto delle differenze e delle peculiarità di ogni Stato.

Costituita da 48 articoli, la Convenzione è suddivisa in quattro capitoli:

- uso dei termini;

[13] Per doppia incriminazione si intende un principio regolatore in materia di estradizione. Tale principio prevede che il fatto posto in essere dall'estradando sia penalmente illecito sia per l'uno che per l'altro Stato, indipendentemente dal fatto che sia indicato con lo stesso nomen iuris nell'ordinamento dei due Stati. Si veda, in tal senso, art. 13 secondo comma del codice penale : "*L'estradizione non è ammessa, se il fatto che forma oggetto della domanda di estradizione, non è preveduto come reato dalla legge italiana e dalla legge straniera*".

[14] J. Clough, "A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonisation", in *Monash University Law Review 2014*, pp 701:
"*Although any international response to cybercrime must therefore seek to accommodate and reconcile these differences, it must be emphasised that 'harmonised' does not mean 'identical*'".

- provvedimenti da adottare a livello nazionale;
- cooperazione internazionale;
- disposizioni finali.

L'obiettivo di armonizzare la disciplina interna degli Stati nella lotta ai Cybercrimes emerge sin da subito.

Il primo capitolo, comprendente un solo articolo, definisce la terminologia che sarà utilizzata nel testo della Convenzione.

In particolare, l'art 1 CCC mira ad armonizzare le nozioni di sistemi informatici, dati informatici, fornitori di servizi e i dati relativi al traffico, in ossequio alla logica per la quale il modo più efficace di regolamentare la Rete consiste nella previsione di regole giuridiche che ne informino gli aspetti tecnici[15].

Il Trattato sulla criminalità informatica di Budapest è il veicolo per la realizzazione dell'ambizioso tentativo di creare legislazioni armonizzate e, per mezzo delle sue disposizioni, cerca di fornire un quadro normativo esauriente, imbattendosi in questioni di ordine sostanziale, procedurale e di cooperazione internazionale[16].

[15] Convenzione di Budapest, art. 1*: "Ai fini della presente Convenzione:*
a. "sistema informatico" indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati;
b. "dati informatici " indica qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione;
c. "service provider" (fornitore di servizi), indica:
1. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico;
2. qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio;
d. "trasmissione di dati" indica qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio".

[16] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40.

3.1 Questioni di ordine sostanziale. Presupposti.

La prima parte della Convenzione si imbatte in questioni di ordine sostanziale. Il secondo capitolo è suddiviso in due sezioni. La prima, '*Diritto Penale Sostanziale*', contiene un elenco delle varie fattispecie di crimini informatici e consta di una serie di previsioni volte a imporre agli Stati membri l'inserimento, nell'ordinamento interno, di specifiche norme di diritto penale sostanziale.

Preliminarmente occorre distinguere le condotte delittuose strettamente connesse alle nuove tecnologie (comportamenti che sono attuabili solo attraverso l'uso di strumenti informatici) dai crimini cd. tradizionali portati a termine in chiave tecnologica (per i quali l'uso di strumenti informatici è funzionale al raggiungimento dello scopo).

La Convenzione introduce '*reati armonizzati*' per eliminare i problemi di doppia incriminazione e migliorare i mezzi per prevenire e reprimere la criminalità informatica.

L'elenco ha come riferimento le linee guida sviluppate dalla Raccomandazione n.° (89) 9 del Consiglio d'Europa sulla criminalità informatica e il lavoro di altre organizzazioni internazionali pubbliche e private (OCSE, ONU, AIDP).

I crimini informatici, molti dei quali già previsti nella citata Raccomandazione del 1989, sono classificati in quattro categorie:

- reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici;
- reati informatici;
- reati relativi al contenuto;
- reati contro la proprietà intellettuale e diritti collegati.

Le disposizioni della Convenzione non si applicano solo ai reati in essa definiti, che si possono denominare '*cibernetici in senso proprio*', ma anche a tutti i reati commessi mediante un sistema informatico, nonché a qualsiasi altro reato di cui si debbano o possano raccogliere "prove in forma elettronica" (art. 14, paragrafo 2 ed art. 23 CCC). Questi reati possono definirsi cibernetici '*in senso improprio*' dato che sono

potenzialmente comprensivi di qualsivoglia fattispecie delittuosa, anche non realizzata nel cyberspace[17].

Inoltre, per la maggior parte delle fattispecie criminose è prevista anche la repressione del tentativo dall'art. 11, paragrafo 2 CCC, ai sensi del quale le Parti devono definire, nelle legislazioni interne, come reato "*il tentativo di commettere ogni tipo di reato in base agli articoli da 3 a 5, 7, 8, 9.1 a. e c. della presente Convenzione"*[18].

Non tutti i reati vengono puniti a titolo di tentativo ma solo quelli indicati dalla presente disposizione. Conseguentemente i reati in essa non richiamati sono puniti solo se consumati, in ragion del fatto che vi sono alcune fattispecie concettualmente difficili da tentare, come ad esempio quella prevista dall'articolo 9.1 lett. b. ossia "*l'offerta o la messa a disposizione di pornografia infantile attraverso un sistema informatico".*

Tutti i reati indicati dalla Convenzione vengono puniti anche a titolo di concorso, ai sensi dell' articolo art. 11, paragrafo 1 CCC. Sarà in tal modo perseguibile penalmente ogni forma di complicità, purché sia commessa intenzionalmente, ossia con la consapevolezza di concorrere alla commissione di una fattispecie di reato.

La Convenzione prevede anche una disciplina sulla responsabilità (penale, civile, amministrativa) delle persone giuridiche. L'art. 12 CCC statuisce che le persone giuridiche sono responsabili per i reati commessi da una persona che riveste una posizione di leadership, nell'esercizio di poteri di rappresentanza, o da una persona che ha un'autorità tale da assumere decisioni o esercitare un controllo. Per configurarsi responsabilità, i soggetti indicati devono aver compiuto uno dei reati previsti dal Trattato; è inoltre richiesto che il reato sia stato commesso per conto e a vantaggio della persona giuridica stessa[19].

---

[17] L. Picotti, Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale, in *Diritto dell'internet,* n. 2/2005, p. 197.

[18] Convenzione di Budapest, art. 11, paragrafo 2:
"*Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso volontariamente, il tentativo di commettere ogni tipo di reato in base agli articoli da 3 a 5, 7,8,9.1 a. e c. della presente Convenzione".*

[19] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par.124-125.

Allo stesso modo, vi sarà responsabilità della persona giuridica qualora la condotta riprovevole è stata posta in essere, alle medesime condizioni, da un dipendente, cioè da un soggetto che agisce sotto l'autorità e il controllo del leadership.
Infine, l'art. 13 CCC è una disposizione strettamente collegata all'elenco dei reati contenuti nel Trattato di Budapest. In esso è stabilito che le sanzioni da adottare da parte dei vari Stati devono essere effettive, proporzionate e dissuasive e, nel caso di persona fisica, potranno consistere anche in pene detentive.
Analizzando i presupposti, si noti come i singoli reati della Convenzione sulla cyber criminalità previsti dagli articoli da 2 a 10 richiedono, come elementi costitutivi della fattispecie, che la loro commissione avvenga, da un punto di vista oggettivo, '*without right*', ossia senza diritto, e da un punto di vista soggettivo '*intentionally*', cioè intenzionalmente[20].
Bisogna soffermarsi sul significato di queste espressioni. La prima clausola rimanda a quei comportamenti posti in essere in violazione di regole giuridiche extrapenali, per i quali non sia presente una causa di giustificazione (quali il consenso dell'avente diritto, la legittima difesa, lo stato di necessità): senza diritto inteso come senza autorità legislativa, esecutiva, amministrativa, giudiziaria, contrattuale o consensuale. Essa conferisce elasticità alle incriminazioni, senza porre agli Stati limitazioni per la relativa implementazione a livello interno. Esistono quindi atti che, se autorizzati ed eseguiti dalle autorità statali, non saranno considerati reato ai sensi della Convenzione.
La locuzione 'intenzionalmente', invece, esige che il fatto sia sorretto dal dolo, il cui contenuto varia da Stato a Stato. In alcuni casi è richiesta, quale parte integrante dell'incriminazione, un'intenzione specifica. Quest'ultima deve essere intesa nell'accezione che nel nostro ordinamento viene data al dolo specifico (a titolo esemplificativo, l'art. 8 in materia di frode informatica prevede, come elemento costitutivo della fattispecie, il fine di procurare un vantaggio economico).

[20] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 38- 39.

3.1.1 Reati contro la riservatezza, integrità e disponibilità di dati e sistemi informatici

Questa prima categoria comprende reati la cui natura riprovevole è strettamente legata all'ambiente informatico in cui vengono commessi.

Il danno reale o potenziale causato da queste violazioni non deve essere sottovalutato: irrompere in un sistema informatico e introdurre dei virus può causare danni irreparabili a interi database mondiali a causa dell'interconnessione delle reti.

L'accesso illegale trova disciplina all'art. 2 della Convenzione[21].

Questa disposizione punisce la condotta di chi, senza autorizzazione e intenzionalmente, accede all'intero sistema informatico o a parte di esso; una Parte ha la facoltà di punire la condotta di chi viola le "*misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico".*

I due elementi fondamentali sono il dolo e l'abusività dell'azione, mentre sono elementi ulteriori quelli che riguardano i fini illeciti del reperimento delle informazioni e la violazione delle misure di sicurezza che le proteggevano[22].

La penalizzazione del mero accesso, cioè hacking, cracking o violazione del computer, deriva dalla necessità di prevenire la commissione di fattispecie di reato più gravi, elencate negli articoli successivi. Infatti, tali intrusioni consentono la conoscenza di dati riservati (password, account , etc.) che potrebbero incoraggiare i crackers a commettere attacchi molto più pericolosi, come ad esempio frodi informatiche.

[21] Convenzione di Budapest, art. 2 "Accesso illegale":
"*Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per sanzionare come reato in base alla propria legge nazionale l'accesso all'intero sistema informatico o a parte di esso senza autorizzazione. Una Parte può richiedere che il reato venga commesso violando misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico*".

[22] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 44-50

L'intercettazione illegale trova disciplina nell'art 3 della Convenzione[23]. Questa disposizione mira a proteggere la privacy dei dati, sulla scia della disciplina relativa alle intercettazioni e registrazioni di conversazioni telefoniche nel mondo fisico.

La norma tutela il diritto alla riservatezza dei dati informatici nella fase della loro trasmissione. Non si tratta della riservatezza personale o epistolare, dato che la stessa previsione prescinde da un siffatto contenuto dei dati, ma della riservatezza informatica, così come si evince dalla provenienza o presenza dei dati all'interno di un sistema informatico o dalla modalità di condotta, la quale deve avvenire per mezzo di strumenti tecnici.

Le intercettazioni devono essere compiute senza diritto, cioè senza autorizzazione, intenzionalmente e tramite trasmissioni '*non pubbliche*' di dati digitali fra due sistemi informatici. 'Non pubblico' qualifica la natura del processo di trasmissione dei dati e non la natura degli stessi.

In particolare, ci si riferisce a qualsiasi processo chiuso rispetto alle intromissioni esterne, ossia alla volontà delle parti che comunicano di farlo in maniera assolutamente personale e non con la possibile aggiunta di altri soggetti.

La disposizione prevede che alcuni Paesi possano chiedere, per il configurarsi della fattispecie, un elemento ulteriore rispetto all'intenzione e all'assenza di autorizzazione: che il reato sia commesso con intento illegale o in relazione ad un sistema informatico connesso ad altro sistema informatico[24].

La Convenzione incrimina le due fattispecie di *attentato all'integrità dei dati* (art. 4 CCC) *e dei sistemi* (art. 5 CCC).

---

[23] Convenzione di Budapest, art. 3 "Intercettazione illegale":
"*Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale l'intercettazione senza autorizzazione, fatta con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche da un sistema informatico che ha tali dati informatici. Una Parte può richiedere che il reato venga commesso con intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico.".*

[24] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 51-59.

Con la prima, vengono punite condotte di danneggiamento, cancellazione, deterioramento, modifica o soppressione di dati informatici[25]. Anche in relazione a questo reato sono richiesti, come requisiti oggettivi e soggettivi, l'assenza di autorizzazione e l'intenzione, considerando che gli operatori di sistema spesso possono avere il diritto di tenere tali condotte, senza l'intenzione di arrecare alcun danno.

La norma elenca dettagliatamente tutte le possibili condotte illecite costituenti reato: il PC-CY, al momento della stesura della Convenzione, ha tenuto in considerazione le norme di ogni Stato, al fine di non creare vuoti normativi a livello sovranazionale e per questo tende ad essere ridondante o ad utilizzare sinonimi o ripetizioni di concetti.

Alle parti è data facoltà di esigere che la condotta causi un danno grave; la gravità va interpretata in relazione alla legislazione nazionale dello Stato che si avvale di questo ulteriore requisito. Lo scopo perseguito dalla norma è assicurare ai dati informatici la stessa protezione di cui godono gli oggetti materiali contro i danni intenzionali.

L'art. 5 CCC punisce le stesse condotte individuate nella disposizione che lo precede[26]. Tali comportamenti, tuttavia, non hanno ad oggetto il semplice dato, ma l'intero sistema informatico. Il bene protetto è l'interesse dei fornitori dei servizi e degli utenti al corretto funzionamento dei sistemi informatici.

Contrariamente all'interferenza dei dati, per configurarsi reato è necessario che la condotta pregiudizievole costituisca un ostacolo al funzionamento del sistema connotato dal requisito della gravità.

Ciascuno Stato, sulla base del proprio diritto interno, deve stabilire quando un impedimento può essere considerato grave.

---

[25] Convenzione di Budapest, art. 4 "Attentato all'integrità dei dati":
"1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici senza autorizzazione.
2. Ogni Parte può riservarsi il diritto di richiedere che la condotta descritta nel paragrafo 1. sia di grave danno.".

[26] Convenzione di Budapest, art. 5 "Attentato all'integrità di un sistema":
"Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale il serio impedimento, senza alcun diritto, del funzionamento di un sistema informatico tramite l'introduzione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatico".

La Convenzione ha introdotto una nuova figura di reato rispetto a quelle previste nelle Raccomandazioni che l'hanno preceduta: *l'abuso di dispositivi* (art. 6 CCC)[27].

Essa comporta una forte anticipazione della soglia di rilevanza penale, rispetto all'effettiva causazione non solo di un danno, ma anche di un mero pericolo per i beni giuridici protetti dalle disposizioni finora considerate[28].

La norma incrimina sia gli atti posti in essere per compiere successivamente un accesso abusivo, sia quelli necessari per un'operazione di danneggiamento informatico. La punibilità ha carattere generale, dato che mira a colpire "*la fabbricazione, la vendita, l'importazione o altra forma di messa a disposizione di un dispositivo, compreso un programma informatico, o di una password e, addirittura, anche il semplice possesso di questi elementi*".

La scelta della Convenzione è una via di mezzo fra le due possibilità estreme di incriminare soltanto dispositivi di per sé illeciti e come tali concepiti fin dall'origine; ovvero qualsiasi dispositivo utilizzabile, di fatto, anche per fini non leciti.

---

[27] Convenzione di Budapest, art. 6 "Abuso di dispositivi":
"*1 Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commessi intenzionalmente e senza autorizzazione:*
a. la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o l'utilizzabilità in altro modo di:
1. un'apparecchiatura, incluso un programma per computer, destinato o utilizzato principalmente al fine di commettere un qualsiasi reato in base agli articoli da 2 a 5 di cui sopra;
2. una password di un computer, un codice d'accesso, o informazioni simili con le quali l'intero sistema informatico o una sua parte sono accessibili, con l'intento di commettere qualsiasi reato in base agli articoli da 2 a 5 di cui sopra;
b. il possesso di uno elemento di cui ai sopra citati paragrafi a. 1. o 2., con l'intento di utilizzarlo allo scopo di commettere qualche reato in base agli articoli da 2 a 5. Una Parte può richiedere per legge che vi sia il possesso di un certo numero di tali elementi perché vi sia una responsabilità penale.
2. Questo articolo non va interpretato nel senso di prevedere una responsabilità penale laddove la produzione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o l'utilizzazione in altro modo o il possesso di cui al paragrafo 1. di questo articolo, non avvenga allo scopo di commettere un reato in base agli articoli da 2 a 5 di questa Convenzione, come anche per il collaudo autorizzato o la protezione di un sistema informatico.
3. Ogni Parte può riservarsi il diritto di non applicare il paragrafo 1. di questo articolo, purché tale riserva non concerna la vendita, la distribuzione o l'utilizzazione in altro modo degli elementi riferiti al paragrafo 1 a. 2. di questo articolo.".

[28] L. Picotti, Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale, *in Diritto dell'internet,* 2005.

In quest'ultima ipotesi si sarebbe corso il rischio di un penalizzazione eccessiva, che avrebbe potuto estendersi ad ogni dispositivo 'a doppio uso' (lecito ed illecito), come ad esempio quelli per testare la sicurezza di un sistema. Mentre la loro esclusione avrebbe ristretto troppo la portata dell'incriminazione.
Il problema è stato risolto con la previsione secondo la quale le predette condotte devono, in ogni caso, essere realizzate con l'intenzione specifica ('ulteriore' rispetto a quella generalmente richiesta per tutti i reati), che detti dispositivi o password, "siano utilizzati al fine di commettere" una delle ipotesi incriminate ai sensi degli artt. da 2 a 5.
Desta qualche perplessità la scelta di affidarsi ad un elemento meramente finalistico (il dolo specifico dell'agente) e ad una locuzione normativa che implica un giudizio di prevalenza circa la destinazione dei dispositivi e programmi in questione, che devono essere 'principalmente' concepiti od adattati a scopi illeciti, al fine di determinare il confine fra lecito ed illecito penale.
Sicuramente il legislatore nazionale dovrebbe meglio precisare tali requisiti, stabilendo una soglia più determinata anche sotto il profilo della 'pericolosità' del fatto punibile.

3.1.2 Reati informatici

La categoria dei reati informatici comprende la *falsificazione informatica* e la *frode informatica.*
Si tratta di comportamenti manipolatori in entrambi i casi. Essi rappresentano la versione informatica dei reati tradizionali di truffa e di falsificazione di documenti, perpetrati nel mondo fisico.
L'art. 7 della Convenzione riproduce, con alcune modifiche, la formulazione di cui alla lettera b della lista minima della Raccomandazione del Consiglio d'Europa del 1989 e definisce la Falsificazione informatica come "*una serie di condotte, di alterazione, introduzione, possesso o soppressione di dati, poste in essere con l'intenzione di creare*

dati non autentici e di utilizzarli o considerarli come se fossero autentici ai fini legali" [29].

Non è necessario che i dati siano o meno direttamente leggibili ed intellegibili: l'immissione nel sistema di un dato errato crea una situazione analoga alla creazione di un documento falso. I dati informatici oggetto dalla norma sono quelli che hanno un contenuto 'probatorio', sia in ambito pubblico che privato. L'interesse protetto è la genuinità delle prove e la sicurezza dei dati elettronici che hanno rilevanza per la regolamentazione legale dei rapporti sociali.

La parte finale dell'articolo in esame prevede che le parti, nel perseguimento di tale crimine possano richiedere, quale ulteriore requisito per l'insorgere della responsabilità penale, che il fatto sia commesso con intento fraudolento o illegale.

La disposizione ha un ampio raggio operativo poiché, sia nel settore privato che in quello pubblico, si assiste alla proliferazione di documentazione giuridicamente rilevante prodotta in forma elettronica.

L'art. 8 CCC in tema di *frode informatica* analizza due tipi di condotta illecita: la manipolazione dei dati digitali e l'interferenza nel funzionamento di un sistema informatico[30].

Lo scopo della disposizione è perseguire penalmente qualsiasi manipolazione indebita nel corso del trattamento dei dati, con l'intenzione di ottenere un trasferimento illegale di proprietà; si mira a colmare le lacune nel diritto penale relative alla "*falsificazione*

[29] Convenzione di Budapest, art. 7 "Falsificazione informatica":
"*Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commessi intenzionalmente e senza alcun diritto, l'introduzione, l'alterazione, il possesso o la soppressione di dati informatici derivanti da dati non autentici con l'intento che essi siano presi in considerazione o utilizzati con fini legali come se fossero autentici, senza avere riguardo al fatto che i dati siano o meno direttamente leggibili o intelligibili. Una Parte può richiedere che il reato venga commesso fraudolentemente, o con un intento illegale paragonabile, perché vi sia una responsabilità penale."*

[30] Convenzione di Budapest, art. 8 "Frode informatica":
"Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso intenzionalmente e senza alcun diritto, il cagionare un danno patrimoniale ad altra persona: a. con ogni introduzione, alterazione, cancellazione o soppressione di dati informatici; b. con ogni interferenza nel funzionamento di un sistema informatico, con l'intento fraudolento o illegale di procurare, senza alcun diritto, un beneficio economico per se stesso o altri".

tradizionale", che richiede la leggibilità visiva di dichiarazioni e non può trovare applicazione in relazione a dati che vengono archiviati elettronicamente.
I comportamenti incriminati sono quelli di introduzione, alterazione, cancellazione o soppressione di dati informatici o di interferenza nel funzionamento di un sistema informatico.
L'evento consumativo consiste nell'aver causato, oggettivamente, un "*danno patrimoniale ad altri*". Sul piano soggettivo occorre, oltre all'intenzionalità del fatto, lo specifico intento di ottenere "senza diritto" un vantaggio economico, per sé o per altri.

3.1.3 Reati relativi al contenuto

La disposizione di cui all'art. 9 CCC, occupa l'intera categoria dei reati relativi al contenuto[31].
L'ambito dei reati relativi al contenuto è stato successivamente esteso con l'introduzione di un protocollo aggiuntivo alla Convenzione, sottoscritto a Strasburgo nel 2003,

[31] Convenzione di Budapest, art. 9 "Pornografia infantile":
"*1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesse intenzionalmente e senza alcun diritto:*
a. la produzione di pornografia infantile allo scopo della sua diffusione attraverso un sistema informatico; b. l'offerta o la messa a disposizione di pornografia infantile attraverso un sistema informatico;
c. la distribuzione o la trasmissione di pornografia infantile attraverso un sistema informatico;
d. il procurare pornografia infantile attraverso un sistema informatico per se stessi o altri; e. il possesso di pornografia infantile attraverso un sistema informatico o uno strumento di archiviazione di dati informatici.
2. Ai fini del Paragrafo 1. di cui sopra, l'espressione "pornografia infantile" include il materiale pornografico che raffigura:
a. un minore coinvolto in un comportamento sessuale esplicito;
b. un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito;
c. immagini realistiche raffiguranti un minore coinvolto in un comportamento sessuale esplicito;
3. Ai fini del Paragrafo 2. di cui sopra, il termine "minore" include tutte le persone sotto i 18 anni di età. Una Parte può comunque richiedere un'età minore, che non potrà essere inferiore ai 16 anni.
4. Ogni Parte può riservarsi il diritto di non applicare in tutto o in parte il paragrafo 1., sottoparagrafi d. ed e., e 2, sottoparagrafi b.e c.".

il quale incrimina condotte di natura razzista e xenofoba commesse tramite sistemi informatici.

Al fenomeno della violenza sessuale diretta sui minori si affianca quello del mercato clandestino di materiale pornografico realizzato attraverso lo sfruttamento sessuale degli stessi. Tale mercato desta particolare interesse, considerato l'enorme volume d'affari che riesce a generare attraverso l'utilizzo della Rete Internet e delle nuove tecnologie informatiche.

Con la direttiva 2011/92/UE del Parlamento Europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, l'Unione europea ha esplicitamente affermato che:

"*(...) l'abuso e lo sfruttamento sessuale dei minori, compresa la pornografia minorile, costituiscono gravi violazioni dei diritti fondamentali, in particolare del diritto dei minori alla protezione e alle cure necessarie per il loro benessere, come sancito nella Convenzione delle Nazioni Unite sui diritti del fanciullo del 1989 e nella Carta dei diritti fondamentali dell'Unione europea (art. 34) (...)*"[32].

Per mezzo di questa direttiva il legislatore comunitario ha fornito una definizione di pornografia minorile, eliminando qualsivoglia interpretazione:

"*La pornografia minorile comprende spesso la registrazione di abusi sessuali compiuti sui minori da parte di adulti. Essa può anche comprendere immagini di minori coinvolti in atteggiamenti sessuali espliciti o immagini dei loro organi sessuali, ove tali immagini siano prodotte o utilizzate per scopi prevalentemente sessuali, indipendentemente dal fatto che siano utilizzate con la consapevolezza del minore. Inoltre, il concetto di pornografia minorile comprende altresì immagini realistiche di un minore in atteggiamenti sessuali espliciti o ritratto in atteggiamenti sessuali espliciti, per scopi prevalentemente sessuali*"[33].

Gli Stati adottano a livello interno, una serie di misure volte alla protezione dei soggetti minori di età. Tuttavia è emersa la necessità di uno strumento internazionale in grado

[32] Gazzetta ufficiale dell'Unione europea, 17/12/2011, L. 335/1, consultabile al sito web https://eur-lex.europa.eu/legalcontent/IT/TXT/PDF/?uri=CELEX:32011L0093&from=IT

[33] Ibidem.

di fronteggiare il problema della negoziazione di materiale pornografico nel Cyberspazio.

Premesso ciò, il Consiglio d'Europa attribuisce ai reati relativi alla pornografia infantile la massima importanza

È stata considerata una questione politica importante quella di impostare uno standard internazionale uniforme per stabilire quando si verifica il raggiungimento della maggiore età.

La Convenzione statuisce che il minore è il soggetto che non ha compiuto i 18 anni di età, così come stabilito anche dall'art. 1 della Convenzione delle Nazioni Unite sui diritti dei fanciulli.

Le parti hanno la facoltà di stabilire un'età inferiore, purché questa non sia inferiore ai 16 anni.

La nozione di pornografia infantile comprende: il materiale pornografico che raffigura un minore in un comportamento sessualmente esplicito (art. 9, par. 2, lett. a CCC), la pornografia virtuale (art. 9, par. 2, lett. c CCC) e quella apparente (art. 9, par. 2, lett. b CCC).

Quest'ultima è costituita da "*immagini realistiche rappresentanti un minore impegnato in un comportamento sessualmente esplicito*", senza che sia realmente coinvolto. La prima concerne, invece, "*una persona che appaia come un minore impegnato in un comportamento sessualmente esplicito*" [34].

Gli interessi tutelati saranno, a loro volta, differenti. Nella prima ipotesi, l'interesse tutelato sarà la protezione del minore dallo sfruttamento strumentale alla produzione di materiale pornografico. Nelle altre due ipotesi muta sia l'interesse tutelato che il grado di offensività: l'esigenza è quella di contrastare comportamenti 'pericolosi' che

[34] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 100. Per " comportamento sessuale esplicito" deve intendersi: A 'sexually explicit conduct' covers at least real or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It is not relevant whether the conduct depicted is real or simulated.

incoraggerebbero al reclutamento di minori a detti fini, nel quadro di una sottocultura favorevole al loro sfruttamento[35].
Tali illeciti devono essere posti in essere, da un punto di vista oggettivo, "*senza diritto*" e, da un punto di vista soggettivo, "*intenzionalmente"*.
Le condotte si differenziano in:

- condotte da incriminare obbligatoriamente, anche a titolo di tentativo, senza poter essere oggetto di opzioni o riserve da parte degli Stati aderenti[36]. Tra queste rientrano: "*la produzione di pornografia minorile in vista della sua diffusione tramite un sistema informatico*" (art. 9, par.1, lett. a) e "*la diffusione o la trasmissione di pornografia minorile tramite un sistema informatico"* (art. 9, par. 1, lett. c);

- condotte che devono essere obbligatoriamente incriminate, ma non anche a titolo di tentativo. Tra queste rientrano: la semplice "*offerta o messa a disposizione di pornografia minorile tramite un sistema informatico"* (art. 9, comma 1, lett. b). Si fa riferimento alla modalità di circolazione dei dati nella rete, che si realizza attraverso la loro 'messa a disposizione' in siti o spazi accessibili agli utenti, che sono posti di fronte alla possibilità di scaricarli (download) su propri computer e supporti o comunque di visualizzarli[37];

- condotte che consistono nel "*procurarsi o procurare ad altri pornografia minorile tramite un sistema informatico"* (art. 9, comma 1, lett. d) e nel "*possedere pornografia minorile in un sistema informatico o in un mezzo di memorizzazione di dati informatici*"(art. 9, comma 1, lett. e). L'incriminazione di tali comportamenti, non puniti a titolo di tentativo, è suscettibile di riserva . La ratio di tale

[35] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par.102.
[36] Convenzione di Budapest, art. 9, par.4.
[37] L. Picotti, op. cit. p. 64.

disposizione è eliminare alla radice il problema della domanda di materiale pornografico da parte del pubblico.

3.1.4 Reati contro la proprietà intellettuale e diritti collegati

La categoria dei reati contro la proprietà intellettuale e diritti collegati comprende le fattispecie di *"violazione del diritto d'autore e diritti connessi"*. Si tratta di un campo particolarmente sensibile allo sviluppo tecnologico.

L'art. 10 CCC non contiene una formulazione dettagliata delle condotte punibili, ma rinvia alla legislazione di ogni Stato aderente, attuativa delle obbligazioni già assunte in forza di strumenti internazionali in materia di *"diritti di proprietà intellettuale"* (art. 10, comma 1) e di *"diritti connessi"* (art. 10, comma 2). Restano escluse, invece, le violazioni concernenti i brevetti ed i marchi, in quanto non esplicitamente trattate dalla Convenzione[38].

La scelta della Convenzione di menzionare anche questo settore di violazioni '*estremamente frequenti*' in Internet deriva dalla facilità di riproduzione e circolazione non autorizzata di opere tramite mezzi informatici.

È sancito un obbligo minimo di incriminazione penale corrispondente a quello nascente dalla sottoscrizione di altri strumenti internazionali, richiamati dalla norma. Questi sono: l'Atto di Parigi del 24 luglio 1971 della Convenzione di Berna per la protezione delle opere letterarie e artistiche, l'Accordo sugli Aspetti commerciali dei diritti di proprietà intellettuale (TRIPS), i due Trattati dell'Organizzazione Mondiale per la Proprietà Intellettuale (OMPI), rispettivamente sulla proprietà intellettuale e sulle interpretazioni, esecuzioni e fotogrammi, la Convenzione di Roma per la protezione degli artisti, interpreti ed esecutori, produttori di fonogrammi e organismi di radiodiffusione.

Dalla lettura della disposizione in esame si evince che il minimo fissato dalla Convenzione in materia è la previsione che le violazioni devono essere dolose[39].

Sempre in ossequio a tale norma è stabilito che le sanzioni penali devono obbligatoriamente intervenire solo per contrastare violazioni commesse '*su scala commerciale*',

[38] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 109.

[39] Più correttamente la norma parla di "*atti commessi deliberatamente*", sulla scia di quanto previsto dall'art. 61 Accordo TRIPS.

fermo restando alla discrezionalità degli Stati la scelta d'incriminare, eventualmente, anche altre tipologie di violazioni della proprietà intellettuale.

4. Il diritto processuale convenzionale: principi generali

La Convenzione di Budapest del 2001 reca, in conformità alle esigenze di armonizzazione e di cooperazione rafforzata che la connotano, un vero e proprio statuto processuale ad hoc destinato a essere implementato negli Stati aderenti.
La seconda sezione disciplina le misure procedurali, vale a dire le metodologie di indagine che devono essere seguite nella lotta ai crimini: così come il diritto penale sostanziale si è progressivamente adeguato alle peculiarità dei crimini informatici, allo stesso modo anche il diritto processuale ha dovuto tenere il passo agli sviluppi della tecnologia.
La parte procedurale della Convenzione deriva da un delicato esercizio di redazione. In effetti, è stata oggetto di un maggiore controllo e anche di maggiori critiche; critiche sollevate soprattutto in relazione al suo rapporto con la protezione dei diritti individuali, a causa di una forte tensione tra la necessità di migliorare le capacità di contrasto al crimine, tramite strumenti procedurali ad hoc, e la tutela delle libertà individuali e della privacy, così come riconosciuta da tempo.
Il diritto processuale convenzionale è costituito da regole comuni che devono essere adottate dagli Stati nello svolgimento delle indagini informatiche.
Gli artt. 14-22 della Convenzione introducono, accanto alle misure procedurali tradizionali della perquisizione e del sequestro, seppur adattate al nuovo contesto tecnologico, una disciplina che mira alla conservazione dei dati e al loro ottenimento in vista di procedimenti penali.
Grazie a queste procedure sarà possibile avvalersi delle diverse tipologie di poteri investigativi, nel caso in cui un reato sia commesso mediante un sistema informatico; sarà inoltre possibile raccogliere prove elettroniche, utili, sia nel perseguimento dei reati elencati dalla Convenzione, sia in relazione ad altri tipi di reato in cui tali prove hanno un ruolo fondamentale.

Potranno essere sequestrati dati e i soggetti che li posseggono potranno essere obbligati alla loro divulgazione e conservazione fino al termite delle indagini ma, in nessun caso, la Convenzione potrà essere considerata uno strumento che giustifichi un sistema '*Orwelliano'* di sorveglianza elettronica[40].

La necessità di garantire il corretto svolgimento delle procedure non può richiedere né giustificare, una sorveglianza sistematica delle comunicazioni o dei contatti personali da parte dei fornitori di servizi o delle forze dell'ordine, a meno che non sia necessario ai fini di una specifica indagine ufficiale[41].

I primi due articoli della Convenzione, in ambito procedurale, attengono al piano dei principi: stabiliscono regole generali relativamente all'azione da portare avanti nel compimento di un'indagine informatica[42].

L'art. 14 della Convenzione prevede che ciascuno Stato è obbligato ad adottare le misure legislative e di altro tipo che possono essere necessarie, in conformità con il suo diritto interno e quadro giuridico, per stabilire i poteri e le procedure descritte nella Convenzione, allo scopo di indagini o procedimenti penali specifici[43].

Al paragrafo 2 è individuato l'ambito di applicazione delle disposizioni procedurali. Esse troveranno applicazione nel perseguimento dei reati stabiliti dalla Convenzione (artt. 2-11), di altri reati commessi mediante un sistema informatico, e nella raccolta delle prove in forma elettronica di un reato. Alla regola sono previste due eccezioni.

---

[40] G. Ilarda e G. Marullo, op. cit. p. 45, pp.22: "*The text concerns only specific criminal investigations and cannot be used, as some people seem to suspect, to set up a widespread "Orwellian" system of electronic surveillanc"*.

[41] Da allora, tale obbligo è stato imposto da varie leggi nazionali (es. USA PATRIOT Act) e, a livello di Unione Europea, dalla Direttiva 2006/24 / CE del 15 marzo 2006 sulla conservazione dei dati generati o elaborati in connessione con la fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58 / CE. La presente direttiva imporrà ai fornitori di servizi Internet e alle compagnie telefoniche di conservare i dati su ogni messaggio elettronico inviato e telefonata effettuata per un periodo compreso tra sei mesi e due anni al fine di garantire che tali dati siano disponibili ai fini delle indagini, dell'individuazione e del perseguimento di gravi criminalità.

[42] Sarzana C., Ippolito S., Informatica, in *Internet e diritto penale*, cit. p. 600.

[43] Convenzione di Budapest, art. 14 par. 1 "Ambito di applicazione delle disposizioni procedurali": *"*1. *Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire i poteri e le procedure previste in questa Sezione per indagini o procedimenti penali specifici"*.

La prima è da ricondurre alla clausola di riserva che "*salvo una disposizione contraria prevista dall'art. 21 CCC*". Quest'ultimo prevede che l'intercettazione dei dati è limitata alle infrazioni penali considerate 'gravi', così come stabilito dal diritto interno di ogni Stato membro: molti Stati scelgono di limitare questo potere così invasivo, al fine di tutelare il diritto alla privacy.

La seconda eccezione, prevista dall'art. 14 CCC, riguarda la raccolta in tempo reale di dati sul traffico, la cui disciplina si trova all'art. 20 CCC. Tale raccolta può essere limitata, a discrezione della Parte, solo ai reati indicati dalla legislazione della Parte stessa (tramite una riserva), poiché considerata un'invasione della sfera di privacy dei soggetti.

Tuttavia per l'esercizio di questa facoltà è stabilita una condizione: l'ambito dei reati interessati da questa riserva non deve essere più ristretto rispetto ai reati per i quali è ammessa l'intercettazione di dati ai sensi dell'art. 21 CCC.

Considerata l'importanza assunta da tale meccanismo procedurale, utile per l'individuazione della fonte o della destinazione delle comunicazione (quindi all'individuazione dei criminali), la Convenzione invita gli Stati a limitare il più possibile la riserva.

La disposizione procedurale principale della Convenzione di Budapest è l'articolo 15 CCC, in materia di "garanzie e condizioni"[44].

[44] Convenzione di Budapest, art. 15 "Condizioni e tutele":
"1. Ogni Parte deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di proporzionalità.
2. Quando sia il caso, avuto riguardo alla natura del potere o della procedura, queste condizioni e tutele devono includere, fra l'altro, una supervisione giudiziaria o di altra natura purché indipendente, dei motivi che giustifichino l'applicazione e la limitazione del campo di applicazione e della durata del potere o procedura.
3. Nella misura in cui ciò sia rispondente all'interesse pubblico e, in particolare, alla buona amministrazione della giustizia, ogni Parte deve considerare l'impatto dei poteri e delle procedure di questa sezione sui diritti, le responsabilità e gli interessi legittimi dei terzi".

La relazione esplicativa aiuta nella complessa impresa di interpretazione della previsione in commento.

Essa è una disposizione di protezione generale: prevede che tutte le procedure elencate, nella sezione seconda della Convenzione, siano soggette alle condizioni e alle tutele previste dal diritto interno di ciascuna Parte.

Il riferimento è ai tradizionali poteri di perquisizione e sequestro (articoli 18 e 19 CCC) e alle eventuali disposizioni esistenti in materia di intercettazione di telecomunicazioni (articoli 20 e 21 CCC).

La norma chiede alle Parti di ispirarsi al loro diritto processuale penale nazionale e di considerare nuovi strumenti garantisti, a seconda della natura del potere che implementano.

Sebbene gli Stati siano obbligati a introdurre le disposizioni processuali convenzionali nel loro ordinamento, le modalità di implementazione e di inserimento sono lasciate alla libera determinazione della legislazione nazionale. La Convenzione si applica, infatti, a diversi sistemi e diverse culture giuridiche e non è possibile specificare, in dettaglio, le condizioni e le garanzie relative ad ogni potere o procedura.

Nell'implementazione ogni Stato dovrà tener conto dei diritti umani e delle libertà, nonché dei diritti che derivano dagli obblighi contratti in base alla "Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali"[45], al "Patto internazionale sui diritti civili e politici"[46] e ad altri strumenti internazionali applicabili in tema di diritti umani.

A titolo esemplificativo, l'art. 17 dell'ICCPR statuisce che:

"*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*".

[45] *Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, aperta alla firma 4 Novembre 1950, 213 UNTS 221 (entrato in vigore il 3 settembre 1953) ("*ECHR*").

[46] *Patto internazionale sui diritti civili e politici*, aperto alla firma il 16 dicembre 1966, 999 UNTS 171 (entrato in vigore il 23 marzo 1976) ("*ICCPR*").

Nessuno potrà subire delle interferenze arbitrarie o illegali nella propria sfera privata e, nel caso ciò si verifichi, sarà compito della legge garantire adeguata protezione[47].
Tutto ciò deve avvenire in conformità del principio di proporzionalità, ossia di quel principio secondo il quale i poteri di indagine devono essere adeguati alla natura e alle circostanze del reato: tutte le misure compiute nei riguardi dell'imputato devono essere strettamente limitate a quanto necessario per lo svolgimento dell'indagine[48].
Nell'adeguamento del diritto interno alle previsioni procedurali convenzionali e in modo compatibile con "*l'interesse pubblico*" e "*la buona amministrazione della Giustizia"*, le Parti devono considerare ulteriori fattori quali l'impatto del potere o della procedura sui *"diritti, responsabilità e interessi legittimi di terzi",* inclusi i fornitori di servizi, e se possibile, adottare mezzi appropriati per mitigare l'impatto.

4.1 Segue: Gli strumenti di indagine convenzionali

I meccanismi procedurali che trovano disciplina nel Trattato sono:

- conservazione accelerata dei dati informatici memorizzati;
- conservazione accelerata e divulgazione parziale dei dati sul traffico;
- ordine di produzione;
- perquisizione di sistemi informatici;
- sequestro di dati informatici memorizzati;
- raccolta in tempo reale di dati informatici;
- intercettazione dei dati relativi ai contenuti.

I poteri di conservazione rapida di dati informatici immagazzinati o relativi al traffico sono descritti agli art. 16 e 17 CCC.

[47] Art. 15 della Convenzione di Budapest.
[48] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 146.

È previsto che i Paesi adottino misure legislative che consentano alle autorità di ordinare alle persone o alle imprese di fornire informazioni, o di ottenere la protezione rapida di dati in un sistema informatico.

Queste previsioni hanno ad oggetto dati che sono nella disponibilità degli operatori, come ad esempio, i fornitori di servizi: trattasi, infatti, di contenuti "*memorizzati mediante un sistema informatico*", il che presuppone che i dati esistano, siano stati raccolti e siano già stati archiviati

Il primo potere di conservazione si esercita se i dati richiesti sono particolarmente vulnerabili alla perdita o alla modifica, ma il custode dei dati è affidabile, come ad esempio un'azienda rispettabile[49].

In tali situazioni l'integrità dei dati è protetta più rapidamente tramite un ordine di preservazione. A titolo esemplificativo, un fornitore di servizi Internet (in lingua inglese, Internet service provider, in sigla ISP, anche abbreviato in provider) offre agli utenti, tramite la sua organizzazione e dietro la stipulazione di un contratto di fornitura, servizi inerenti al web, come l'accesso al World Wide Web e la posta elettronica. Le forze dell'ordine possono costringere un ISP a conservare tutti i dati relativi a qualsiasi indagine, in particolare se il rischio di perdita è alto.

L'ISP è tenuto a preservare i dati per un *"periodo di tempo adeguato",* presumibilmente finché l'indagine delle forze dell'ordine è in corso.

---

[49] Convenzione di Budapest, art 16 "Conservazione accelerate dei dati informatici memorizzati":
"*1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle competenti autorità di ordinare o ottenere in altro modo la protezione rapida di specifici dati informatici, inclusi i dati sul traffico, che sono stati conservati attraverso un sistema informatico, in particolare quando vi è motivo di ritenere che i dati informatici siano particolarmente vulnerabili e soggetti a cancellazione o modificazione.*
2. Quando una Parte rende effettive le previsioni di cui al precedente paragrafo 1. attraverso l'ordine ad un soggetto di conservare specifici dati informatici immagazzinati che siano in suo possesso o sotto il suo controllo, la Parte deve adottare le misure legislative e di altra natura che siano necessarie per obbligare tale soggetto a proteggere e mantenere l'integrità di quei dati informatici per il periodo di tempo necessario, per un massimo di novanta giorni, per consentire alle autorità competenti di ottenere la loro divulgazione. Una Parte può prevedere che tale ordine possa essere successivamente rinnovato.
3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per obbligare il custode o la persona incaricata di conservare i dati informatici di mantenere il segreto sulla procedura intrapresa per il periodo di tempo previsto dal proprio diritto interno.
4. I poteri e le procedure di cui al presente articolo devono essere soggetti agli articoli 14 e 15".

L'articolo impone ulteriormente agli Stati di adottare leggi che contengano l'ordine, diretto alla persona che preserva i dati, di mantenere il segreto sulla procedura per il periodo di tempo previsto dalla legislazione nazionale. In altre parole, un ISP nel fornire dati su richiesta delle forze dell'ordine deve farlo entro un certo periodo di tempo e non deve rendere pubblica alcuna informazione relativa alle indagini.

Il potere di conservazione previsto all'art. 17 CCC consente alle forze dell'ordine di risalire alla fonte di una comunicazione, nel caso in cui più fornitori siano stati coinvolti nella sua trasmissione; il fine è identificare altri fornitori di servizi coinvolti nella trasmissione di comunicazioni specifiche oggetto di indagine[50].

Altra misura procedurale introdotta dalla Convenzione è quella prevista dall'art. 18 CCC, rubricato "*ingiunzione di produrre*"[51].

---

[50] Convenzione di Budapest, art. 17, "Conservazione e divulgazione rapida dei dati relativi al traffico":
"1. *Al fine di assicurare la conservazione dei dati relativi al traffico in applicazione di quanto previsto all'articolo 16 ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per:*
a. assicurare che la conservazione dei dati relativi al traffico sia disponibile nonostante uno o più fornitori di servizi siano stati coinvolti nella trasmissione di tale comunicazione;
b. assicurare la rapida trasmissione all'autorità competente della Parte, o al soggetto designato da tale autorità, di una quantità di dati relativi al traffico sufficiente per consentire alla Parte di identificare il fornitore di servizi e la via attraverso la quale la comunicazione fu trasmessa.
2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15".

[51] Convenzione di Budapest, art. 18 "Ingiunzione di produrre":
"1. *Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle autorità competenti di ordinare:*
a. ad un soggetto nel proprio territorio di trasmettere specifici dati informatici nella propria disponibilità o controllo, che siano immagazzinati in un sistema informatico in un supporto informatico per la conservazione di dati; e
b. a un fornitore di servizi che offre le proprie presatazioni nel territorio della Parte di fornire i dati in proprio possesso o sotto il suo controllo relativi ai propri abbonati e concernenti tali servizi.
2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.
3. Ai fini del presente articolo, l'espressione "informazioni relative agli abbonati" designa ogni informazione detenuta in forma di dato informatico o sotto altra forma da un fornitore di servizi e relativa agli abbonati ad un proprio servizio e diversa dai dati relativi al traffico o al contenuto e attraverso la quale è possibile stabilire:
a. il tipo di servizio di comunicazione utilizzato, le disposizioni tecniche prese a tale riguardo e il periodo del servizio;
b. l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio;
c. ogni altra informazione sul luogo di installazione dell'apparecchiatura della comunicazione, disponibile sulla base degli accordi o del contratto di fornitura del servizio".

Il fine è ottenere informazioni rilevanti per le indagini penali.

Anziché chiedere agli Stati di applicare misure coercitive nei confronti di soggetti terzi, come la ricerca e il sequestro dei dati, è essenziale che essi dispongano, a livello interno, di poteri investigativi alternativi, che rappresentino un mezzo meno intrusivo rispetto a quelli appena citati.

La relazione esplicativa sottolinea che "*un ordine di produzione fornisce una misura flessibile che le forze dell'ordine possono applicare in molti casi, soprattutto come misura alternativa a misure più invadenti o più onerose. L'attuazione di tale meccanismo procedurale sarà vantaggiosa anche per i soggetti che custodiscono i dati, come gli ISP, che sono spesso pronti ad assistere le autorità, su base volontaria, fornendo i dati sotto il loro controllo, ma che preferiscono una base giuridica appropriata per tale assistenza, in modo da essere sollevati da qualsiasi responsabilità contrattuale o extracontrattuale*"[52].

L'ingiunzione mira alla produzione, ordinata dalle autorità competenti, di dati che si trovano nella disponibilità di privati.

Oggetto sono i '*dati sugli abbonati'*: informazioni gestite da un ISP riguardanti gli abbonati, sia dal punto di vista del contratto con essi stipulato o del servizio sottoscritto, sia da quello delle generalità (identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio).

L'articolo si riferisce ai dati già presenti all'interno degli archivi elettronici e richiede ai provider una collaborazione minimale, consistente solo nella messa a disposizione di dati archiviati precedentemente al fine di favorire le indagini.

Gli artt. 19 - 21 sono il cuore delle disposizioni procedurali.

I poteri relativi alla perquisizione dei sistemi informatici e al sequestro dei dati memorizzati (art. 19 CCC) sono l'equivalente informatico delle tradizionali analoghe disposizioni nell'ambiente tangibile[53].

[52] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 171.

[53] Convenzione di Budapest, art. 19 "Perquisizione e Sequestro dei dati immagazzinati":

La ricerca di prove informatiche nel nuovo ambiente tecnologico conserva molte delle caratteristiche inerenti alla ricerca di prove tradizionali.

Per esempio, la raccolta dei dati avviene durante il periodo della ricerca e ha come oggetto dati esistenti in quel momento, proprio come avviene per le prove relative agli oggetti tangibili. I presupposti per ottenere l'autorizzazione legale, al fine di intraprendere la ricerca, rimangono gli stessi, vale a dire la convinzione che tali dati esistano e forniscano la prova di un illecito.

Notevoli sono le differenze: in primo luogo, i dati sono in forma intangibile; in secondo luogo, i dati digitali possono essere letti con l'uso di apparecchiature informatiche e, a differenza degli omologhi tradizionali, non possono essere sequestrati e portati via alla stregua di un documento cartaceo; inoltre, a causa della connettività dei sistemi informatici, i dati potrebbero trovarsi in un archivio esterno collegato direttamente o indirettamente al computer attraverso la Rete.

"1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di perquisire o accedere in modo simile:
a. a un sistema informatico o parte di esso e ai dati informatici ivi immagazzinati; e
b. a supporto per la conservazione di dati informatici nel quale i dati stessi possono essere immagazzinati nel proprio territorio.
2. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire che, qualora le proprie autorità perquisiscano o accedano in modo simile a specifici sistemi informatici o parte di essi, in conformità al paragrafo 1.a, e abbiano ragione di ritenere che i dati ricercati si trovino presso un altro sistema informatico o parte di esso nel proprio territorio, e a tali dati sia possibile legalmente l'accesso dal sistema iniziale, le stesse autorità possano estendere rapidamente la perquisizione o l'accesso all'altro sistema.
3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di sequestrare o acquisire in modo simile i dati informatici per i quali si è proceduto all'accesso in conformità ai paragrafi 1 o 2. Tali misure devono includere il potere di:
a. sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici;
b. fare e trattenere una copia di quei dati informatici;
c. mantenere l'integrità dei relativi dati informatici immagazzinati;
d. rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato.
4. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati informatici in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie per consentire l'applicazione delle misure di cui ai paragrafi 1. e 2.
5. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15".

Sorge la necessità di regole che consentano un'estensione della ricerca al luogo in cui i dati sono effettivamente memorizzati[54]. Questa necessità sta alla base della disposizione in esame.

La perquisizione 'convenzionale', infatti, è progettata per garantire la consultazione e la ricerca dei dati informatici da parte delle autorità competenti interessate. Queste attività hanno ad oggetto i dati contenuti all'interno di un sistema informatico o parte di esso (come un dispositivo di archiviazione dati collegato) o su un supporto di archiviazione dati indipendente (come un CD-ROM o un dischetto).

Il sequestro 'convenzionale' consente alle autorità di sequestrare o proteggere i dati informatici che sono stati perquisiti o a cui si è avuto accesso.

È ammesso il sequestro dell'hardware del computer e dei supporti di memorizzazione dei dati del computer.

Nella Convenzione il termine 'sequestrare' significa togliere il supporto fisico su cui sono registrati i dati o le informazioni, o conservarne una copia; implica anche l'uso o il sequestro dei programmi necessari per accedervi.

La disposizione in esame, al paragrafo 4, introduce una misura coercitiva. Quest'ultima è necessaria per facilitare la perquisizione e il sequestro laddove è difficile accedere ad un sistema a causa della quantità di dati che possono essere elaborati e conservati, e della natura delle operazioni informatiche.

Tale misura prevede la possibilità di consultare soggetti con particolari conoscenze e competenze in ambito informatico, riguardo alle modalità tecniche relative all'esperimento delle misure investigative.

La ratio è l'efficienza della ricerca, la quale va a vantaggio delle autorità, delle aziende colpite, nonché degli abbonati ai servizi forniti da quest'ultime: le autorità investigative, infatti, potrebbero rimanere nei locali perquisiti e impedire l'accesso al sistema informatico per lunghi periodi di tempo durante la ricerca, con conseguenze negative sull'intera attività.

[54] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 186-187.

In controtendenza, gli articoli 20 e 21 CCC trattano della raccolta e dell'intercettazione in tempo reale di dati, e non della mera conservazione o raccolta di dati già in possesso di qualcuno.

Essi ammettono la possibilità per l'autorità competente "*di raccogliere o registrare dati attraverso l'utilizzo di strumenti tecnici nel suo territorio*"; inoltre prevedono la possibilità di obbligare un fornitore di servizi, nell'ambito delle sue capacità tecniche, a "*raccogliere o registrare dati attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte*" o "*cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati relativi al contenuto di comunicazioni specifiche eseguite nel proprio territorio attraverso un sistema informatico*"[55].

I due articoli sono praticamente identici. Gli unici elementi distintivi sono i dati oggetto delle disposizioni.

I dati che possono essere individuati, tramite raccolta e intercettazione, sono di due tipi: rispettivamente '*dati sul traffico'* e '*dati sul contenuto'*.

Nell'articolo 1 lett. d CCC, per 'dati sul traffico' si intende qualsiasi dato informatico relativo a una comunicazione realizzata per mezzo di un sistema informatico, generato dal sistema e che costituisce una parte della catena di comunicazione, grazie alla quale

[55] Convenzione di Budapest, art. 20 "Raccolta in tempo reale di dati sul traffico:
"*1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di:*
a. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici nel suo territorio;
b. obbligare un fornitore di servizi, nell'ambito delle sue capacità tecniche a:
i. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel suo territorio, o
ii. cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati sul traffico associati a comunicazioni specifiche effettuate sul proprio territorio attraverso un sistema informatico.
2. Qualora una Parte, a causa dei limiti previsti dal proprio ordinamento giuridico, non è in grado di applicare le misure previste al paragrafo 1.a, può, invece, adottare le misure legislative o di altra natura che dovessero essere necessarie per consentire la raccolta o la registrazione in tempo reale dei dati relativi al traffico associati a comunicazioni specifiche effettuate sul proprio territorio, attraverso l'utilizzo di strumenti tecnici esistenti su questo territorio.
3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare un fornitore di servizi a mantenere segreti il fatto che un qualsiasi potere previsto nel presente articolo sia stato esercitato e ogni informazione relativa. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15".

è possibile individuare origine della comunicazione, destinazione, percorso, ora, data, dimensioni e durata o tipo di servizio.

Cosa si intende per 'dati di contenuto' non è specificato nella Convenzione. In via interpretativa, si fa di riferimento al contenuto della comunicazione, cioè al significato o lo scopo, il messaggio o le informazioni trasmesse dalla stessa.

Infine, in entrambi i casi, si tratta di strumenti invasivi, che sollevano molte problematiche relative al rispetto del diritto alla riservatezza delle comunicazioni e, in generale, interferiscono con il diritto alla privacy.

Per quel che concerne poi l'intercettazione dei dati di contenuto, la Convenzione prevede che gli Stati contraenti sono tenuti a utilizzare tale procedura solo "*in relazione a una serie di reati gravi che devono essere determinati dal diritto interno*"[56].

I redattori della Convenzione non sono stati in grado di concordare alcun obbligo per gli Stati che gli imponesse di includere i crimini informatici nell'elenco nazionale dei reati 'gravi', e dunque intercettabili.

Pertanto, l'ambito di applicazione di questa disposizione è lasciato alla discrezionalità nazionale (ad esempio, l'Italia non ha esercitato questa facoltà, quindi le intercettazioni

[56] Convenzione di Budapest, art. 21 "Intercettazione di dati relativi al contenuto":
"*1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie, in relazione ad una serie di gravi infrazioni che devono essere definite dal diritto nazionale, per consentire alle proprie competenti autorità di:*
a. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, e
b. obbligare un fornitore di servizi, nell'ambito delle sue capacità tecniche a:
i. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, o
II. cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati relativi al contenuto di comunicazioni specifiche eseguite nel proprio territorio attraverso un sistema informatico. 2. Qualora una Parte, a causa dei principi del proprio ordinamento giuridico, non è in grado di applicare le misure previste al paragrafo 1.a, può invece adottare misure legislative e di altra natura che dovessero essere necessarie per assicurare la raccolta o la registrazione in tempo reale dei dati relativi al contenuto di comunicazioni specifiche eseguite sul proprio territorio, attraverso l'utilizzo di strumenti tecnici in quel territorio.
3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare un fornitore di servizi a mantenere segreto il fatto che un qualsiasi potere previsto nel presente articolo sia stato sia stato esercitato e ogni informazione relativa.
4.I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15".

possono essere avviate per indagini in merito a qualsiasi fattispecie criminosa commessa in relazione a sistemi informatici)[57].

[57]G. Ilarda e G. Marullo, op.cit. p. 45, pp.24.

5. La cooperazione: i principi

La capacità di svolgere indagini che interessano il territorio di altri Stati, ovvero la cosiddetta '*giurisdizione investigativa*'[58], trova disciplina nel capitolo III della Convenzione, capitolo dedicato alla cooperazione internazionale e composto dalla previsione di principi generali a cui seguono disposizioni specifiche.

Ogni Stato emana norme che disciplinano nuove fattispecie di reati informatici e che prevedono nuovi meccanismi procedurali per il perseguimento degli stessi. Tuttavia, nel momento in cui queste procedure dovranno essere applicate al di fuori del territorio nazionale l'accordo tra le parti diventerà di importanza cruciale.

La cooperazione ha l'obiettivo di ridurre, a livello internazionale, gli ostacoli al flusso di informazioni per consentire alle forze dell'ordine di svolgere indagini per conto di altri Stati e trasmettere il materiale probatorio con maggiore rapidità.

Norma cardine in materia di cooperazione internazionale è l'art 23 della Convenzione. Il fine della disposizione è estendere i rapporti cooperativi agevolando lo scambio di informazioni e prove telematiche, le cd. *'digital evidence'*:

"*Le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti i reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione internazionale in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale"*[59].

[58] United Nations Office on Drugs and Crime, '*Comprehensive Study on Cybercrime',* https://www.unodc.org/unodc/en/organizedcrime/comprehensivestudyoncybercrime.

[59] Convenzione di Budapest, art. 23 "Principi generali relative alla cooperazione internazionale": "Le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti i reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma

Essa contiene tre principi generali:

- La Convenzione esordisce affermando che la cooperazione tra gli stati deve essere favorita "*nella misura più ampia possibile*". Questo principio richiede alle Parti di fornire un'ampia cooperazione reciproca e di ridurre al minimo gli ostacoli al flusso regolare e rapido di informazioni e prove a livello internazionale[60].

- La cooperazione deve essere estesa a tutti i reati relativi ai sistemi informatici, ai dati, nonché alla raccolta di prove in forma elettronica relative a qualsiasi reato. Troveranno applicazione le disposizioni del capitolo III sia quando il reato è commesso mediante l'uso di un sistema informatico, sia quando si tratta di un reato ordinario non commesso mediante l'uso di un sistema informatico (ad esempio un omicidio), ma nel perseguimento del quale acquistano rilevanza prove elettroniche.
- Le procedure di scambio devono avvenire nel rispetto e secondo le modalità previste dalla Convenzione e, inoltre, in applicazione degli accordi internazionali di cooperazione in materia penale, delle leggi reciproche e anche delle singole norme già vigenti negli ordinamenti degli Stati. Da ciò si evince il principio secondo cui le norme della Convenzione sulla cooperazione non devono sostituire quelle degli altri strumenti internazionali[61].

Le tecniche cooperative mirano a coordinare le azioni dei vari Paesi nei settori dell'estradizione e dell'assistenza reciproca.
L'estradizione comporta la consegna formale di una persona da parte di uno Stato ad un altro Stato, al fine di perseguirlo penalmente o per l'imposizione o l'esecuzione di una pena, ed è comunemente supportata da trattati bilaterali. Prerogativa della misura

elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione internazionale in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale*"*.
[60] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 242.
[61] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 243.

è la '*doppia criminalità*': per essere estradabile il reato deve essere un "reato" ai sensi delle leggi di entrambe le giurisdizioni. Questo principio è emerso in tempi sufficientemente recenti, al fine di tutelare l'esigenza della reciprocità e delle pari sovranità delle sfere giurisdizionali tra gli Stati cooperanti nei loro rapporti di diritto internazionale.

Le difficoltà a cui si va incontro in caso di mancanza di doppia incriminazione sono ben illustrate dal noto caso di un virus rinomato *'Love Bug'.* Il virus è apparso per la prima volta a Hong Kong nel 2000 e poi si è diffuso rapidamente in tutto il mondo. Ha colpito le principali società, tra cui Ford, Siemens e Microsoft, nonché agenzie governative, NASA e CIA. È stato stimato di aver interessato oltre 45 milioni di utenti in più di venti paesi, causando danni per miliardi di dollari.

Molti utenti ricevettero una e-mail, contenente la seguente frase: *'controlla la mia lettera d'amore in allegato'*. Tuttavia, l'allegato conteneva uno script dannoso che infettava i file della vittima appesantendo il computer e inserendosi nella rubrica dei contatti. Il risultato fu un'ondata virale di messaggi, che nel giro di poche ore causò congestioni dei sistemi, poiché il virus informatico non si limitava ad auto replicarsi, ma rinominava e cancellava anche molti dei file contenuti nei computer delle vittime.

Sebbene gli investigatori fossero in grado di individuare il responsabile, un ex informatico studente nelle Filippine, tale condotta non poteva essere punita perché il paese di origine non aveva leggi applicabili in materia e, dunque, non poteva essere estradato negli Stati Uniti a causa di mancanza di doppia criminalità[62].

L'esempio mostra che la ricerca dell'uomo che ha creato il virus sarebbe stata più rapida ed efficace, qualora fossero esistite leggi comuni e armonizzate sulla criminalità informatica tra i Paesi interessati, in particolare nel paese da cui ha avuto origine il virus.

L'estradizione causa non poche problematiche, dato che una giurisdizione potrebbe riconoscere come reato una condotta che non è tale per un altro ordinamento. Anche in presenza di un Trattato tra due Stati, le problematiche potrebbero sorgere qualora quest'ultimo elencasse in via enumerativa le condotte estradabili e non in maniera

[62] J. Clough, *Principles of cyber crime*, 2010, pp. 471.

prescrittiva, oppure qualora i reati elencati non comprendessero nuove forme di illecito informatico[63].

In questo scenario si colloca la Convenzione, la quale cerca di fornire regole generali volte al superamento di queste problematiche.

L'art. 24 enuncia i principi e regole fondanti l'estradizione. Il fine è rendere effettivo quest'istituto, in osservanza del principio di diritto internazionale '*aut dedere aut judicare*' (obbligo di estradare o perseguire) [64]. Esso disciplina i casi in cui alcuni Paesi siano favorevoli all'estradizione mentre altri no, lasciando un margine decisionale abbastanza ampio agli Stati[65].

---

[63] J. Clough, op. cit. p. 53.

[64] Principio del diritto internazionale in forza del quale lo Stato sul cui territorio si trova un autore di crimini internazionali ha l'obbligo di sottoporlo a giudizio o di estradarlo.

[65] Convenzione di Budapest, art. 24 "Estradizione":

"*1. a. Il presente articolo si applica all'estradizione tra Parti per i reati stabiliti in base agli articoli da 2 a 11 della presente Convenzione, a condizione che essi siano punibili in base alla legge di entrambe le Parti con la privazione della libertà per un periodo massimo di almeno un anno, o con una pena più severa.*

b. Qualora sia richiesta una pena minima differente in base ad un trattato di estradizione applicabile fra due o più parti, ivi compresa la Convenzione Europea d'Estradizione (STE No. 24) o in forza di un accordo stipulato sulla base di legislazioni uniformi o reciproche, si applica la pena minima prevista in base a questi trattati o accordi.

2. I reati descritti al paragrafo 1 del presente articolo devono essere considerati come inclusi nel novero dei reati che possono dar luogo ad estradizione in tutti i trattati di estradizione esistenti tra le Parti. Le Parti si impegnano ad includere tali reati fra quelli che possono comportare l'estradizione in ogni trattato di estradizione che sarà concluso tra di esse.

3. Qualora una Parte condizioni l'estradizione all'esistenza di un trattato e riceva una richiesta di estradizione di un'altra Parte con la quale non ha un trattato di estradizione, la presente Convenzione può essere considerata come base giuridica per l'estradizione nei riguardi di tutti i reati menzionati al paragrafo 1 del presente articolo.

4. Le Parti che non condizionano l'estradizione all'esistenza di un trattato devono considerare i reati menzionati al paragrafo 1 del presente articolo come reati che possono dar luogo ad estradizione tra di esse.

5. L'estradizione è soggetta alle condizioni previste dal diritto interno della Parte richiedente o dai trattati di estradizione in vigore, inclusi i motivi in base ai quali la Parte richiesta può rifiutare di concedere l'estradizione.

6. Qualora l'estradizione per un reato menzionata al paragrafo 1 del presente articolo venga rifiutata esclusivamente sulla base della nazionalità della persona ricercata, o perché la Parte richiesta eccepisce la propria competenza per quel reato, la Parte richiesta deve sottoporre il caso su richiesta della Parte richiedente alle proprie autorità competenti a procedere e dovrà trasmettere i risultati finali alla Parte richiedente in tempo utile. Tali autorità dovranno prendere le proprie decisioni e condurre le proprie indagini e i procedimenti allo stesso che per tutti gli altri reati comparabili per natura in base alla legislazione di tale Parte.

7. a. Ogni Parte, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, deve comunicare al Segretariato Generale del Consiglio d'Europa il

In primo luogo, si applica alle infrazioni previste dagli artt. 2-11 della Convenzione e a condizione che siano punibili, nelle legislazioni di entrambi gli Stati, con una pena detentiva massima di almeno un anno o pena più severa; tuttavia, se esiste un Trattato di estradizione o un accordo tra le parti che prevede una pena minima differente, a questa pena occorre fare riferimento. La conseguenza è che, nella pratica, nonostante si sia in presenza di un reato estradabile ai sensi della Convenzione, qualora esso sia punito con una pena inferiore a quella prevista, l'estradizione non sarà concessa.

In secondo luogo, i reati a cui fa di riferimento la norma devono essere considerati sempre estradabili. Ciò non significa che l'estradizione deve essere concessa in ogni occasione, ma piuttosto che lo Stato destinatario della richiesta deve essere disponibile a valutare la possibilità di concederla a soggetti che hanno commesso tali crimini, valutando la sussistenza dei requisiti richiesti[66].

In conformità con il principio generale di cooperazione internazionale, se una Parte condiziona l'estradizione all'esistenza di un Trattato e riceve una domanda di estradizione da un'altra Parte con la quale non ha un Trattato di estradizione, la Convenzione può rappresentare il fondamento giuridico per l'estradizione, purché si tratti di un reato menzionato dagli artt. 2-11 (art. 24 par. 3). Non si tratta di un obbligo ma di una facoltà. Qualora l'estradizione non sia condizionata all'esistenza di un Trattato, le Parti dovranno considerare i reati appena richiamati come reati che possono dar luogo all'estradizione.

Infine il paragrafo 6 stabilisce un obbligo nei confronti di uno Stato che rifiuta di concedere l'estradizione, con la motivazione di averne la competenza a giudicare o qualora il rifiuto dipenda dalla nazionalità della persona ricercata.

Tale obbligo consiste nel sottoporre il caso alle autorità giuridiche competenti dello Stato che ha rifiutato l'estradizione e nel comunicare, nel più breve tempo possibile, i

---

nome e l'indirizzo di ogni autorità responsabile dell'invio o della ricezione delle richieste di estradizione o di arresto provvisorio in mancanza di un trattato.
b. Il Segretariato Generale del Consiglio d'Europa deve istituire e aggiornare un registro delle autorità a tal fine designate dalle Parti. Ogni Parte deve assicurare che i dati del registro siano corretti in ogni momento."

[66] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 247.

risultati allo Stato richiedente. Se non è stata presentata alcuna richiesta di estradizione o se questa è stata negata per motivi diversi dalla nazionalità, la norma non stabilisce alcun obbligo per lo Stato di attivarsi penalmente.

L'art. 25 della Convenzione di Budapest detta i principi generali in materia di mutua assistenza, relativamente al traffico e alla raccolta di dati e di prove informatiche, nel tentativo di estendere all'estremo limite i rapporti di cooperazione[67].

Tutti gli Stati riconoscono la limitata efficacia dell'assistenza reciproca e, conseguentemente, la necessità di migliorare le procedure di indagine. Nella pratica le misure di assistenza legale reciproca sono considerate complesse, lunghe e dispendiose in termini di risorse.

Sebbene la Convenzione non sia riuscita a risolvere in toto queste problematiche, ha contribuito a migliorare la situazione.

In questa materia, come anche stabilito all'art. 23 della Convenzione in tema di principi generali di cooperazione internazionale, è previsto l'obbligo per gli Stati di collaborare nel modo più ampio possibile, per agevolare le indagini o i procedimenti relativi a

---

[67] Convenzione di Budapest, art. 25 "Principi generali relative alla mutual assistenza":
"1. Le Parti devono concedersi reciprocamente la più ampia mutua assistenza al fine delle indagini o dei procedimenti relativi ai reati relativi a sistemi e dati informatici o per la raccolta di prove in formato elettronico di reati.
2. Ogni Parte deve anche adottare le misure legislative e di altra natura che dovessero essere necessarie per l'adempimento degli obblighi assunti in base agli articoli da 27 al 35.
3. Ogni Parte può, in casi d'urgenza, fare richieste di mutua assistenza o comunicazioni ad essa relative attraverso strumenti rapidi di comunicazione, come il fax o la posta elettronica, a condizione che tali strumenti diano appropriate garanzie di sicurezza e autenticazione (inclusa la criptazione, se necessaria), seguite da conferma ufficiale ulteriore se lo Stato richiesto lo esige. Lo Stato richiesto deve accettare la domanda e rispondere alla richiesta con uno qualsiasi di tali mezzi rapidi di comunicazione.
4. Salva contraria disposizione espressamente prevista negli articoli del presente capitolo, la mutua assistenza è soggetta alle condizioni previste dalla legislazione della Parte richiesta o dai trattati di mutua assistenza applicabili, inclusi i motivi sulla base dei quali la Parte richiesta può rifiutare la cooperazione. La Parte richiesta non può esercitare il diritto di rifiutare la mutua assistenza in relazione ai reati menzionati negli articoli da 2 a 11 per il solo motivo che la richiesta riguarda un reato che essa reputa di natura fiscale.
5. Qualora, in conformità alle previsioni del presente capitolo, la Parte richiesta è autorizzata a subordinare la mutua assistenza ad una doppia incriminazione, questa condizione sarà considerata come soddisfatta, se il comportamento considerato reato per il quale la mutua assistenza è stata richiesta costituisca reato in base al proprio diritto interno, a prescindere dal fatto che la propria legislazione classifichi o meno il reato nella stessa categoria o lo denomini con la stessa terminologia della legislazione della Parte richiedente".

sistemi e dati informatici o raccolta di prove. Le Parti dovranno disporre di una base giuridica per poter realizzare concretamente gli obblighi assunti, in particolare quelli previsti agli articoli da 27 a 35[68].

Analizzando in generale le modalità di assistenza reciproca è previsto che in caso di urgenza (volatilità dei dati, possibili danni imminenti a persone o a cose, ecc.) ciascuna Parte può inoltrare domanda di assistenza mediante mezzi rapidi di comunicazione, ad esempio il fax, il corriere elettronico o altri mezzi tecnologici. Ovviamente tale richiesta deve essere subordinata alla condizione che questi mezzi offrano garanzie sufficienti di sicurezza e di autenticazione (ivi compreso, se necessario, mezzi crittografici). Lo Stato a cui la richiesta è inviata deve accettarla e rispondere per mezzo di strumenti di comunicazione rapida.

Lo scopo di questa previsione è facilitare l'accelerazione del processo di ottenimento di assistenza, in modo tale da evitare il pregiudizio derivante dalla dispersione o eliminazione dei dati prima che la richiesta venga preparata, trasmessa e fornita[69].

La mutua assistenza è regolata dal diritto interno di ogni Stato o dai Trattati di assistenza applicabili, a meno che non sia diversamente stabilito. Con questa clausola di riserva la norma fa di riferimento ad una serie di ipotesi derogatorie della previsione generale, contenute nella stessa Convenzione. A titolo esemplificativo, l'articolo in commento prevede che la cooperazione non può essere negata, per quanto riguarda i reati previsti dagli articoli 2-11 della Convenzione, per il solo motivo che la Parte alla quale è stata fatta la richiesta la considera come avente ad oggetto un reato 'fiscale'.

[68] Si tratta delle disposizioni che disciplinano: le procedure relative alla domanda d'assistenza in assenza di accordi internazionali applicabili (art. 27), alla riservatezza delle informazioni ed alle restrizioni nella loro utilizzazione (art. 28), alla conservazione rapida dei dati informatici raccolti (art. 29), alla divulgazione rapida dei dati conservati (art. 30), all'assistenza concernente l'accesso ai dati raccolti (art. 31), all'accesso transfrontaliero ai dati raccolti con il consenso o quando essi sono accessibili al pubblico (art. 32), all'assistenza nella raccolta in tempo reale dei dati relativi al traffico (art. 33), all'assistenza in materia di intercettazione dei dati relativi al contenuto (art. 34), alla rete denominata 24/7 (art. 35).

[69] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par.256.

La Convenzione del Consiglio d'Europa disciplina entrambe le situazioni in cui un rapporto giuridico tra le Parti in tema di assistenza esista o meno. Laddove vi sia un rapporto preesistente, questo non verrà sostituito dalla Convenzione.

I principi generali terminano con la disposizione di cui al paragrafo 5. La ratio è garantire che la Parte destinataria di una richiesta di mutua assistenza non adotti un test troppo rigido per valutare l'esistenza di doppia incriminazione. Date le differenze nei sistemi giuridici nazionali, infatti, è inevitabile che sorgano variazioni nella terminologia e nella categorizzazione della condotta criminale.

Il caso considerato è quello in cui la Parte che riceve la richiesta di mutua assistenza, prima di prestarla, deve verificare la sussistenza della doppia incriminazione. A tal proposito, è stabilito che la condizione è soddisfatta, con la conseguenza che l'assistenza potrà avvenire, qualora per il diritto interno dello stato che riceve la richiesta il comportamento da incriminare costituisca reato. È indifferente che questo reato abbia lo stesso *nomen juris* di quello dello stato richiedente. L'assistenza è favorita tramite uno standard di doppia incriminazione 'flessibile' capace di adattarsi alle diverse legislazioni[70].

L'assistenza giudiziaria reciproca (MLA) è una delle procedure più importanti tra le misure di contrasto alla criminalità informatica e di altri reati che comportano l'utilizzo di prove elettroniche.

Il Dipartimento di Stato degli Stati Uniti descrive i trattati di assistenza legale reciproca 'MLAT' come mezzo per "migliorare l'efficacia dell'assistenza reciproca e per regolarizzare e facilitare le procedure con le nazioni. I trattati includono tipicamente procedure concordate per convocare testimoni, permettere la produzione di documenti e di altre prove, emettere mandati di perquisizione e procedure di notifica"[71].

Come anticipato, le misure cooperative introdotte dal Trattato riguardano anche forme di assistenza reciproca in assenza di MLAT, (*mutual legal assistance treaty)*[72].

[70] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 259.
[71] Miriam F. Miquelon- Weismann, op. cit. p. 27.
[72] Un trattato di mutua assistenza legale (MLAT) è un accordo tra due o più paesi allo scopo di raccogliere e scambiare informazioni nel tentativo di far rispettare le leggi pubbliche o penali. Una

L'art. 27 CCC contiene previsioni dettagliate relativamente alle situazioni nelle quali non esistono tra le Parti precedenti accordi internazionali applicabili. Innanzitutto le Parti devono designare uno o più autorità centrali incaricate di trasmettere la richiesta di assistenza o di rispondervi, di eseguirle o di trasmetterle alle autorità competenti per la loro esecuzione. Tali autorità comunicano direttamente le une con le altre. La Convenzione precisa che le domande di assistenza nel caso previsto dall'articolo in questione sono eseguite secondo la procedura specifica della parte richiedente, a meno che siano incompatibili con le legislazioni della Parte richiesta. È previsto inoltre che, oltre ai motivi o alle condizioni di rifiuto di assistenza previsti dall'art. 25 par. 4, l'assistenza può essere rifiutata dalla parte richiesta:

- se la richiesta riguarda un reato che la Parte in questione considera come di natura politica o collegato a un reato politico;
- se la Parte ritiene che il fatto di accedere alla richiesta rischi di creare pericoli o di attentare alla sua sovranità, alla sua sicurezza, al suo ordine pubblico o ad altri interessi essenziali.

Inoltre la parte richiesta può sospendere l'esecuzione delle misure se ritiene che tali richieste rischino di pregiudicare inchieste o procedure condotte dalle sue autorità. È previsto un obbligo di informazione della parte richiesta in ordine al seguito che intende dare alle domande di assistenza, motivando eventualmente il rifiuto, e comunque informando la parte richiedente di una qualsiasi ragione che renda impossibile l'esecuzione di assistenza o suscettibile di ritardo.

La parte richiedente può domandare alla parte richiesta che i fatti e l'oggetto dell'inchiesta restino riservate.

In caso d'urgenza, le autorità giudiziarie della Parte richiedente possono indirizzare direttamente ai loro omologhi della Parte richiesta la domanda di assistenza o le comunicazioni relative, informando immediatamente le autorità centrali della parte richiesta.

richiesta di assistenza giudiziaria reciproca viene comunemente utilizzata per interrogare formalmente un sospettato in un procedimento penale, quando il sospettato risiede in un paese straniero.

Ogni richiesta o comunicazione in base al presente paragrafo può essere effettuata attraverso l'Organizzazione Internazionale della Polizia Criminale (INTERPOL).
La Convenzione prevede che in ogni caso le domande o le comunicazioni di cui all'articolo e che non implicano misure coercitive possano essere trasmesse direttamente dalle autorità competenti della Parte richiedente alle autorità competenti della Parte richiesta.

6. Gli strumenti cooperativi in rapporto al principio di sovranità territoriale: le problematiche sollevate dall'art. 32 CCC

La capacità di accesso rapido ai dati posseduti da altre giurisdizioni è un aspetto importante delle moderne indagini penali.
In osservanza del principio di diritto internazionale secondo il quale nessuno Stato può far valere la propria giurisdizione all'interno del territorio di altro Stato sovrano, far rispettare le sue leggi, condurre indagini o arrestare una persona, è considerata violazione della sovranità territoriale la condotta delle forze dell'ordine di portare avanti indagini all'interno di un Paese straniero senza averne l'autorità.
La tecnologia fornisce, tuttavia, alle forze dell'ordine, la capacità di condurre ricerche transfrontaliere, vale a dire "la possibilità di accedere unilateralmente ai dati informatici archiviati da un'altra Parte senza chiedere assistenza reciproca".
La legittimità o meno di queste condotte e la mancanza di tutela per i diritti degli Stati, primo fra tutti quello di sovranità territoriale, sono state oggetto di un acceso dibattito.
Negli anni '80 si propendeva per l'ammissibilità dell'accesso transfrontaliero alle prove elettroniche, poiché all'epoca la questione relativa alle conseguenze negative causate da tali comportamenti non sembrava 'troppo pressante'[73]. Ciò era dovuto alla mancanza di esperienza e alla difficoltà nella formulazione di principi generali applicabili alle diverse circostanze dei casi concreti.

[73] J. Clough, op. ct. p. 719.

Tuttavia, i miglioramenti tecnologici hanno reso la questione più urgente, tanto da essere discussa dal Comitato europeo per i problemi della criminalità, dal G8 e dal Consiglio d'Europa.

Sebbene i redattori della Convenzione abbiano cercato di trovare una soluzione per molto tempo, non è stato possibile accordarsi, ad eccezione di due istanze specifiche, disciplinate all'art. 32 CCC.

La disposizione oggetto di disamina regola due aspetti diversi di accesso transfrontaliero.

Il primo prevede che una parte può, senza l'autorizzazione di un'altra, accedere ai dati del computer archiviati pubblicamente e disponibili, indipendentemente da dove essi si trovino geograficamente. Il secondo, nonché più controverso, è contenuto nell'art 32 lett. b, che consente ad una parte di *"accedere o ricevere, tramite un sistema informatico nel proprio territorio, dati informatici memorizzati che si trovano in un'altra Parte, se la Parte ottiene il legittimo consenso volontario della persona che ha la legittima autorità a rivelare i dati allo Stato attraverso quel sistema informatico"*.

Alcuni Paesi, in particolare la Russia, non hanno condiviso questa disposizione sostenendo che "*potrebbe danneggiare la sovranità*", la sicurezza dei paesi membri e i diritti dei loro cittadini. È evidente che la disposizione in esame presenti criticità. Essa consente, ad esempio, al proprietario di un account di posta elettronica, i cui dati sono memorizzati in un altro Paese, di divulgare volontariamente o consentire l'accesso a tali dati alle forze dell'ordine locali. L'ampiezza potenziale di questa disposizione diventa evidente se si considera che gran parte delle reti di comunicazione e archiviazione dati sono di proprietà privata. Sono previsti, tuttavia, due limiti a tale potere: il consenso deve essere '*volontario*', ossia non deve essere concesso a seguito di costrizione, coercizione o inganno, così come non può essere prestato da minori o persone con deficit cognitivi.

Tuttavia, per le forze dell'ordine di un Paese incoraggiare un cittadino di altra nazionalità ad assisterli nelle indagini può, già in sé, essere violazione della sovranità territoriale. Al fine di risolvere tali problemi, l'articolo 32 lett. b può essere utilizzato solo per

ottenere il consenso di una persona che però si trovi sotto la giurisdizione dello Stato inquirente. Quanto finora esposto trova conferma nel Rapporto esplicativo alla Convenzione[74].

Qualora, invece, la persona che deve prestare il consenso si trovi nel territorio di altro Stato, dovrebbero esserci procedure di mutua assistenza.

Ulteriore limite imposto dalla disposizione in esame è che il consenso volontario sia prestato dalla persona '*legalmente autorizzata*'. In generale, potrebbe essere legalmente autorizzato sia l'utente di un servizio sia il fornitore del servizio stesso. Il consenso prestato deve essere esplicito, quindi la semplice accettazione da parte di una persona dei termini e delle condizioni di un servizio online, al momento del suo utilizzo, non può valere come prestazione esplicita di consenso, anche qualora queste condizioni contengano l'avvertimento che i dati possono essere condivisi con le autorità di giustizia penale[75].

L'articolo 32 lett. b, inoltre, parla di "*dati informatici immagazzinati situati in un altro Stato",* facendo presumere che se ne conosca sempre l'ubicazione: ciò non è sempre vero poiché i moderni sviluppi tecnologici ne consentono lo spostamento immediato, con la conseguenza che non è possibile stabilirne con certezza la posizione.

Per concludere, l'art 32 CCC, nonostante miri ad evitare il ricorso ai Trattati di mutua assistenza legale (MLAT), è una disposizione che determina dei profili di opacità tra la sua applicazione e la sovranità territoriale dei singoli Stati.

La finalità della disposizione in parola consiste nel disegnare una via rapida e semplificata nell'acquisire dati. Infatti, l'accesso è direttamente ottenuto indipendentemente dall'azione dello Stato interessato, il quale deve limitarsi a concederlo in considerazione del fatto che l'obbligo deriva da uno strumento internazionale. Naturalmente tale meccanismo non trova applicazione in relazione a ipotesi per le quali è prevista la richiesta di mutua assistenza ai sensi e in base a questa Convenzione.

---

[74] Ivi p. 87.

[75] Transborder Group, '*Transborder Access and Jurisdiction: What Are the Options*?', Discussion Paper No T-CY (2012)3, Cybercrime Convention Committee, Council of Europe, 6 December 2012.

Nonostante ciò, possono sorgere questioni non indifferenti: ad esempio, cosa succede se il soggetto che possiede i dati non risponde? Come deve essere espresso il consenso? Come deve essere avanzata la richiesta?

È opportuno notare, dunque, come il ricorso al canale tradizionale delle regole generali di assistenza reciproca resta la soluzione più sicura[76].

In prospettiva '*de jure condend*o' e al fine di porre rimedio ai plurimi aspetti problematici della disposizione, potrebbe essere introdotta *una clausola di tutela della sovranità*, come già presente in alcuni accordi internazionali.

Questo tentativo è già stato esperito in passato.

Ad esempio, l'UNTOC (La Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale), all'art. 4, chiede alle Parti di adempiere agli obblighi che incombono in applicazione della presente Convenzione in modo coerente con i principi di uguaglianza sovrana, di integrità degli Stati e quella del non intervento negli affari interni di altri Stati membri[77].

Viene anche enunciato il principio secondo il quale le Parti non possono esercitare la loro giurisdizione in altri Stati e svolgere funzioni riservate esclusivamente, dal diritto interno, alle autorità di tale Stato.

Un simile principio è stato ampiamente discusso dalla riunione dei Ministri della Giustizia e dell'Interno del G8 a Mosca nel 1999, ma non è stato incluso nella Convenzione di Budapest[78].

7. Task force operativa 24 ore su 24, 7 giorni su 7

Le maggiori novità introdotte dalla Convenzione sulla criminalità informatica si rinvengono proprio nella parte relativa alla mutua assistenza.

[76] Il Sole 24 ore, Politica comune sul Cybercrime già operativa in ventidue Stati, in *Guida al Diritto* 2008, 16, pp. 77

[77] UNTOC art 4 (1). See also United Nations Convention against Corruption, opened for signature 9 December 2003, 2349 UNTS 41 (entered into force 14 December 2005)

[78] Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Communiqué, Moscow, 19–20 October 1999.

Sul versante pratico-operativo, il Trattato introduce la disposizione di cui all'art. 35 CCC. Essa prevede la costituzione di una '*task force'*, ovvero un network operativo 24 ore al giorno per sette giorni alla settimana, denominato "*Rete 24 ore su 24, 7 giorni su 7*", creato sotto l'auspicio del G8 nel 1995.

La rete internazionale di controllo della criminalità informatica sorge dalla necessità di mettere in contatto, in modo permanente, gli Stati, al fine di assicurare un'assistenza immediata alle indagini, sia di giorno che di notte. Ogni Stato deve creare punti di contatto che mirino a fornire assistenza accelerata grazie ad attività di consulenza tecnica, di conservazione di dati in base agli art. 29 e 30, acquisizione di prove e localizzazione di sospetti.

Il punto di contatto è discrezionalmente individuato nella struttura esecutiva ritenuta più adeguata da ogni Paese: ad esempio alcune parti contraenti potrebbero collocarlo in un'unita di polizia specializzata in crimini informatici, altri presso l'autorità centrale per l'assistenza reciproca, a condizione che il coordinamento con le altre autorità avvenga rapidamente[79].

In Italia la task force è costituita da una struttura operativa presso il Servizio di polizia postale e delle comunicazioni della Polizia di Stato, con il compito di assicurare assistenza, sia sotto forma di informazioni da dare su richiesta, sia in relazione all'esecuzione di operazione di congelamento di dati e della loro raccolta. Così, se qualcuno vuole contattare le autorità competenti di un altro Paese, ad esempio per richiedere un intervento urgente di conservazione dei dati, può farlo utilizzando questo mezzo rapido, tramite una telefonata o una semplice e-mail.

È importante un chiarimento. Ai sensi dell'art. 27 CCC è possibile utilizzare questa Convenzione come base legale per la mutua assistenza, ove tra le parti non vi sia un accordo di cooperazione. Laddove questo sia presente, troverà applicazione quanto in esso stabilito e le disposizioni interne, se non derogate dalla Convenzione. Questo vuol dire che una richiesta rivolta all'Italia (analogamente si procederà nel caso in cui il nostro Paese sia quello che richiede assistenza) seguirà la via della rogatoria prevista

[79] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par. 300-301.

dalle norme applicabili (ad esempio la Convenzione europea del 1959; il trattato con gli Stati Uniti ecc.).
La task force in questione procederà all'esecuzione delle misure urgenti richieste. Simultaneamente verrà inviata la richiesta formale all'autorità competente (quella giudiziaria, in caso di urgenza, oppure il ministero della giustizia). Questa richiesta formale immediata trova la sua ragion d'essere nella considerazione che "*a un primo esame la richiesta possa risultare non accoglibile, sì da imporre quindi la cessazione di effetti non consentiti; inoltre costituisce la base per operare conformemente alle previsioni della legge interna".*[80]

8. Una valutazione d'insieme della Convenzione

La Convenzione di Budapest è una guida per ciascun Paese nell'elaborazione di una legislazione completa per combattere la criminalità informatica grazie alle misure sostanziali in essa previste, ai poteri procedurali volti a garantire prove elettroniche e alla sua natura di base giuridica per la cooperazione internazionale.
Gli strumenti introdotti dalla Convenzione sollevano molte criticità in relazione ai loro ambiti d'intervento, alcune delle quali ancora irrisolte.
I punti nevralgici possono essere fondamentalmente ricondotti a due aspetti.
In primis, la necessità di bilanciare le esigenze di indagine volte al contrasto della criminalità e la tutela dei diritti fondamentali, primo fra tutti quello della libertà personale.
In secondo luogo, la complessità di svolgere indagini che abbiano ad oggetto prove elettroniche.

[80] Il sole 24 ore, op. cit. p. 90.

8.1 L'approccio della Convenzione alla tutela dei diritti umani: l'art. 15 CCC e le critiche alla c.d. 'armonizzazione flessibile'

L'accesso a Internet costituisce un mezzo di attuazione di molti diritti fondamentali garantiti a vario titolo dall'ordinamento internazionale.

Si tratta del diritto alla libera espressione, del diritto di informazione e del diritto allo sviluppo; d'altro canto, quello di accedere liberamente e senza limitazioni alla Rete potrebbe assumere i connotati di un autonomo diritto fondamentale di ultima generazione[81].

Il diritto di utilizzare le reti internazionali di telecomunicazioni è una forma di attuazione del diritto di formarsi un'opinione, così come previsto dall'art. 19 comma 1 del Patto internazionale sui diritti civili e politici del 1966 e, a livello europeo, dall'art. 10 CEDU, e di esprimerla ed esprimersi, liberamente cercando, ricevendo e diffondendo, attraverso qualsiasi mezzo, informazioni e idee di ogni genere (art. 19 comma 2 del medesimo Patto, nonché, ancora, art. 10 CEDU) o del diritto a partecipare alla vita culturale e godere dei benefici del progresso scientifico e delle sue applicazioni (art. 15 del Patto internazionale sui diritti economici, sociali e culturali del 16 dicembre 1966)[82].

Sebbene questo sia vero, l'utilizzo della rete comporta la nascita di aspetti problematici.

L'altra faccia della medaglia, infatti, è rappresentata dai riflessi dei meccanismi investigativi sulla protezione dei diritti dell'uomo: critico è il momento in cui le indagini invadono la sfera privata dei soggetti coinvolti.

La Convenzione mira a contrastare la criminalità legata agli sviluppi tecnologici, ma a sua volta determina ulteriori criticità: il Trattato consente in modo ufficiale alle forze

[81] Padovani, Musiani e Pavan, Diritti umani nell'età digitale: concetti in evoluzione e norme emergenti nel contesto trans-nazionale, *in Pol. dir., fascicolo monografico su: Diritti e sfera pubblica nell'era digitale,* 2010, 391 ss.

[82] G.M. Ruotolo, *Enciclopedia del diritto,* Giuffrè, 2015.

dell'ordine di utilizzare i metodi di intrusione in esso previsti, con inevitabili ripercussioni sui diritti fondamentali dell'uomo.

Pertanto, privacy e protezione sono entità concettuali inestricabilmente legate tra loro. La necessità è quella di bilanciare interessi diversi: da una parte, migliorare le iniziative di contrasto a questa nuova forma di criminalità informatica e, dall'altra, tutelare i diritti umani e la protezione della privacy.

L'approccio della Convenzione alla tutela dei diritti umani è stato definito di ' *armonizzazione flessibile*'[83]:

"*A model of uniform rule making confined to establishing parameters for acceptable substantive rules, leaving the formulation of procedural due process rules to the cultural peculiarities of each nation*"[84].

Flessibile, poiché costituita da disposizioni uniformi che si limitano a stabilire parametri per regole a carattere sostanziale, e che lascia la formulazione di regole procedurali di giusto processo alle peculiarità culturali di ciascuna nazione.

In quest'ultimo caso il riferimento normativo è l'art.15 della Convenzione di Budapest. Tale disposizione, ampiamente analizzata precedentemente, prevede che nell'esperimento delle indagini sui crimini informatici, prima di applicare le procedure convenzionali, le Parti contraenti devono verificare che siano proporzionate alla natura e alle circostanze del reato in esame. Inoltre, le Parti devono subordinare le procedure all'autorizzazione di un giudice o di ministro, a seconda del paese, al fine di garantirne un giusto utilizzo[85].

Nel far ciò, saranno salvaguardati i diritti dell'uomo e le libertà: la norma richiama espressamente una serie di strumenti internazionali a cui fare riferimento.

Uno tra questi è il Patto Internazionale sui diritti civili e politici, in sigla l'ICCPR, il quale ad esempio, afferma all'art. 17 che "*nessuno deve essere soggetto a interferenze arbitrarie o illegali con la sua privacy, famiglia, casa o corrispondenza, né ad attacchi*

[83] Miquelon-Weismann, op. cit. p. 27.
[84] J. Clough, op. cit. p. 53, pp. 709.
[85] Rapporto esplicativo della Convenzione sulla criminalità informatica, op. cit. p. 40, par.146-147.

illegali al suo onore e alla sua reputazione" e quello che "*tutte le persone hanno diritto alla protezione della legge contro tali interferenze o attacchi"*[86].

Per gli Stati membri del Consiglio d'Europa il principale strumento applicabile è la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nonché la giurisprudenza della Corte europea dei diritti dell'uomo.

Tali questi strumenti devono essere considerati integralmente, anche se particolare attenzione meritano alcune disposizioni. Si tratta dell'art. 5 "*Diritto alla libertà e alla sicurezza*", art. 6 "*Diritto a un equo processo*", art. 7 "*Nulla poena sine lege*" e art. 8 "*Diritto al rispetto della vita privata e familiare*"[87].

Dunque, sebbene un approccio flessibile faciliti il raggiungimento degli obiettivi delle forze dell'ordine, ciò si rivela a scapito del giusto processo e della protezione dei diritti dell'individuo.

Il binomio protezione-privacy, infatti, non è stato esente da critiche: recenti rivelazioni, riguardanti programmi governativi '*quasi orwelliani'* per la raccolta in massa di dati informatici, sottolineano la necessità di garantire un giusto processo ed una tutela effettiva dei diritti nell'ambiente digitale[88].

Tali considerazioni hanno spinto le Nazioni Unite a dichiarare di essere "*preoccupate per l'impatto negativo che la sorveglianza e/o l'intercettazione delle comunicazioni… nonché la raccolta di dati personali, in particolare se effettuata in massa, può avere sull'esercizio e il godimento dei diritti umani*"[89].

---

[86] Art. 17 ICCPR

[87] Art. 8 CEDU "Diritto al rispetto della vita privata e familiare":

" 1. *Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui"

[88] J. Clough, op. cit. p. 53, pp. 708.

[89] The Right to Privacy in the Digital Age, GA Res 68/167, UN GAOR, 68th sess, Agenda Item 69(b), UN Doc A/RES/68/167 (21 January 2014, adopted 18 December 2013). See also Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN HRC, 23rd sess, Agenda Item 3, d UN Doc A/HRC/23/40 (17 April 2013).

Molte sono le associazioni, sia negli Stati Uniti, che in altre nazioni, le quali hanno espresso preoccupazioni circa le misure previste dalla Convenzione poiché "*sproporzionate, distruttive della libertà e una minaccia per i diritti fondamentali*"[90].

Fornendo al governo il potere di curiosare nelle comunicazioni private e monitorare gli utenti si pone in essere una violazione della libertà di espressione e dell'anonimato.

L'articolo 15 è un castello di sabbia[91].

In primis, non è possibile, a priori, valutare se uno Stato abbia provveduto ad attuarlo prendendo come riferimento semplicemente una o più disposizioni del diritto interno o stabilendo una 'lista di controllo', poiché un approccio di questo tipo sarebbe limitante. Le condizioni e le garanzie devono adattarsi non a fattori statici, bensì dinamici, mutevoli nel tempo, come ad esempio la modifica della legislazione, l'evolversi della tecnologia, il mutare della criminalità e altri fattori[92].

A ciò si aggiunga un'ulteriore preoccupazione. La Convenzione non esprime alcuna limitazione alla gravità dei reati sottoposti ai poteri investigativi. Ne deriva che le misure di cui agli artt. 16 - 21 CCC, possono applicarsi, allo stesso modo, a reati gravi o meno gravi. Queste preoccupazioni conformemente a quanto previsto ai sensi dell'art. 15 CCC sono affrontate in base al principio di proporzionalità: di conseguenza spetta alle singole parti, discrezionalmente, stabilire se un comportamento è sufficientemente serio da giustificare l'applicazione di determinati poteri investigativi.

Nonostante l'ambizioso progetto della Convenzione, essa attribuisce troppa responsabilità al diritto interno nel fornire una protezione della libertà personale adeguata.

Il vero *punctum dolens* è la mancanza di linee guida specifiche che permettano un giusto bilanciamento tra repressione e riservatezza.

Tali limiti sono stati portati all'attenzione del presidente Henrik Kaspersen del PC-CY. Il presidente ha dichiarato apertamente:

---

[90] Consiglio d'Europa Cybercrime @ EaP 2018, *Condizioni e garanzie ai sensi dell'articolo 15 della Convenzione sulla criminalità informatica nel partenariato orientale*, maggio 2018

[91] Ryan M.F. Baron, *A critique of the intenational cyber crime treaty*

[92] Ibidem.

"*We cannot find an acceptable international standard in terms of privacy as it applies to this treaty*"[93].

In altri termini, le leggi europee sulla privacy sono così diverse al punto che risulta estremamente complicato trovare uno standard internazionale comune per la protezione della sfera privata[94].

Nonostante i redattori del Trattato erano consapevoli di dover garantire un giusto equilibrio tra gli interessi delle forze dell'ordine e il rispetto dei diritti umani, questa necessità è ampiamente delusa dalla stesura finale del testo della Convenzione.

8.1.1 Possibili soluzioni di bilanciamento tra repressione dei crimini informatici e tutela della privacy

Nel paragrafo precedente si è avuto modo di constatare che le maggiori critiche mosse alla Convenzione derivano dalla introduzione dei poteri procedurali per la ricerca e il sequestro di dati informatici, dalla possibilità di indagare sui crimini informatici al di fuori del proprio Stato e di ricevere assistenza reciproca nelle indagini transfrontaliere, senza specularmente aumentare gli standard di protezione della privacy.

Così come di prioritaria importanza è stata l'introduzione di strumenti per combattere la criminalità, allo stesso modo è necessario incrementare i livelli di protezione della riservatezza delle attività poste in essere nel web.

La misura compensativa avrebbe dovuto avere ad oggetto la tutela della sfera privata di ogni soggetto contro l'invasione da parte di governi, imprese o individui disonesti.

La soluzione ideale al problema sarebbe l'adozione da parte di tutti gli Stati di discipline volte alla protezione degli individui da irragionevoli intrusioni da parte di governi, imprese e individui disonesti: tuttavia è poco pratico credere che ogni Stato adotterebbe concretamente una tale politica.

---

[93] Consiglio d'Europa Cybercrime @ EaP 2018, op. cit. p. 119.

[94] M. Johnston, *US Companies Find EuropÈs Cyber Crime Treaty Too Vague: Americans Fear Individual Countries' Due-Process Laws Could be Violated*, IDG News Service, at http://www.ebusinessworld.com/english/crd_treaty_321309.htm.

La migliore alternativa disponibile potrebbe essere allora la seguente: i redattori dovrebbero garantire una maggiore protezione della privacy negli Stati che dimostrino disponibilità ad adottare un 'sistema informativo' volto alla tutela della sfera personale dei singoli, assicurando alcune garanzie minime[95].

In altri termini, i dati personali vengono richiesti per svariati motivi e il loro utilizzo può, in molti casi, avvantaggiare l'individuo, ma, in tanti altri, danneggiarlo. Pretendere che tali dati, dopo essere stati inseriti in un sistema, vengano rimossi creerebbe un circuito ingestibile, motivo per cui all'individuo dovrebbe essere garantito il diritto di agire contro coloro i quali se ne servino in modo improprio. Le modalità di azione, volte al perseguimento di tali comportamenti intrusivi, dovrebbero in concreto essere stabiliti dal diritto interno.

Per quegli Stati non disposti a garantire tali livelli di informativa, invece, la Convenzione dovrebbe comunque prevedere un minimo di protezione[96].

Nonostante il presidente Henrik Kaspersen abbia sottolineato le difficoltà a cui sono andati incontro i redattori della Convenzione di Budapest circa l'individuazione di uno standard internazionale 'comune' per la protezione della privacy, potrebbe a ciò obiettarsi che il fine non dovrebbe essere uno standard di tutela mondiale, bensì un aumento incrementale del livello di protezione della privacy informativa attualmente fornita da ogni singolo Stato.

In conclusione, e in considerazione di quanto fin qui esposto, sarebbe bastata la presenza nel Trattato di una disposizione in grado di garantire un incremento della privacy informativa per alleviare, anche se non eliminare del tutto, i problemi legati alla protezione privacy[97].

---

[95] DC Kennedy,*Alla ricerca di un equilibrio tra potere della polizia e privacy neltrattato sulla criminalità informatica*, Rich. JL e Tech 3 (2002).

[96] Ibidem.

[97] Ibidem.

8.2 Ulteriori aspetti critici della Convenzione: le prove digitali

Lo strumento internazionale contiene misure cooperative in relazione alla raccolta e conservazione delle prove digitali nel caso in cui si persegua un crimine informatico e qualsiasi altro tipo di reato, ma non risolve le difficoltà di compiere attività investigative in maniera uniforme nei vari ordinamenti.

L'altro aspetto critico dalla Convenzione, infatti, attiene alla complessità di svolgere indagini che hanno ad oggetto prove elettroniche.

Il problema principale è il rischio che l'acquisizione e la conservazione di dati digitali siano scorrette, non solo per le difficoltà insite nella raccolta stessa, bensì per la possibilità che nei vari Paesi vengano adottate procedure e standard disomogenei.

Garantire prove elettroniche è particolarmente impegnativo nel contesto del 'cloud computing', contesto in cui i dati sono distribuiti su più servizi, fornitori, luoghi e giurisdizioni.

Con i poteri di applicazione della legge limitati dai confini territoriali e l'assistenza giudiziaria reciproca spesso non praticabile, le indagini contro la criminalità informatica rischiano di diventare inefficaci[98].

Consapevoli di questi limiti, nel 2017, in seno al Consiglio d'Europa, sono iniziati i lavori preparatori per un nuovo un protocollo aggiuntivo sulla cooperazione internazionale rafforzata e l'accesso alle prove nel cloud, i quali dovrebbero concludersi nel 2021.

I negoziati del Secondo Protocollo aggiuntivo si concentrano su 4 elementi chiave:

- misure per migliorare la cooperazione internazionale tra le forze dell'ordine e le autorità giudiziarie, compresa l'assistenza legale tra le autorità ('assistenza giudiziaria reciproca');
- cooperazione tra autorità e fornitori di servizi in altri Paesi;
- condizioni e garanzie per l'accesso alle informazioni da parte delle autorità di altri Paesi;

[98] Per un maggior approfondimento https://www.ispionline.it/

- altre garanzie, compresi i requisiti di protezione dei dati.

Alexander Seger, durante i negoziati del nuovo protocollo, ha affermato che:
"*prove in relazione a frode, corruzione, omicidio, stupro, terrorismo, abuso sessuale di bambini e, di fatto, qualsiasi tipo di crimine possono assumere la forma di prove elettroniche archiviate su un server da qualche parte nel cloud. Garantire tali prove è necessario per garantire lo Stato di diritto e proteggere la società e gli individui".*
Le prove digitali sono uno strumento sempre più importante in ambito processual-penalistico: la prova tradizionale sta migrando verso un ambiente virtuale; lo stesso può dirsi per i suoi processi di gestione e criteri di ammissibilità rispetto a quelli che regolamentano le prove tradizionali.
L'utilizzo di prove digitali nei tribunali è incrementato considerevolmente nel corso degli ultimi anni.
Alla stregua di ogni altra tipologia di prova utilizzata in giudizio, le informazioni generate, come risultanza di un'indagine informatica forense, devono rispondere agli standards di prove ammesse a giudizio definiti dalla Corte di Giustizia.
Soltanto garantendo uniformità nelle procedure di acquisizione e di conservazione dei dati digitali è possibile assicurare che, nella successiva fase di valutazione da parte del giudice, gli elementi di prova raccolti potranno essere considerati idonei a provare i fatti della causa[99].
Esistono varie enunciazioni per definire una prova digitale. Tra esse ne spiccano due.
La prima formulata dall'International Organization on Computer Evidence (IOCE) secondo la quale la *electronic evidence* è "un'informazione generata, memorizzata e trasmessa attraverso un supporto informatico che può avere valore in tribunale"; la seconda, adottata dallo Scientific Working Group on Digital Evidence (SWGDE), per

[99] S. Conti, La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia, *in Informatica e diritto,* XLI annata, Vol. XXIV, 2015, n. 1-2, pp. 153-164

cui costituisce *digital evidence* "qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale"[100].

La prova informatica o elettronica (la c.d. *digital evidence*) è caratterizzata dal requisito dell'immaterialità, che, a sua volta, determina non pochi problemi: dalla tutela della privacy, alla individuazione dell'organo inquirente territorialmente competente, alla fragilità del dato informatico.

La fragilità è una caratteristica congenita, ossia prescinde da condotte dolose, e può derivare da comportamenti colposi posti in essere da chi interviene su di esse.

Per tale motivo, al fine di poter produrre in giudizio una prova digitale è necessario garantirne l'autenticità e, soprattutto, riuscire a garantire che, dopo la raccolta, il dato informatico non venga manipolato.

A differenza del documento tradizionale di tipo analogico, ossia il mezzo utilizzato per incorporare la rappresentazione del fatto in una base materiale, il documento informatico prescinde dal tipo di supporto fisico su cui è fissato il dato, ed in ogni momento può essere prelevato e trasferito su altro supporto idoneo a recepirlo[101].

La peculiarità del dato informatico di alterarsi o modificarsi, anche autonomamente, impone agli investigatori un'attenzione particolare ogniqualvolta si proceda ad una perquisizione o ad un sequestro di un sistema informatico.

Prioritaria è l'adozione di particolari tecniche informatiche per garantire e tutelare l'integrità del dato, in vista di non alterare quella che si può definire una vera e propria 'scena criminis informatica'.

Tali risultati possono essere raggiunti attraverso un preciso protocollo che deriva dalle migliori metodologie, '*Best practices',* sperimentate nella prassi investigativa internazionale[102].

---

[100] Soluzioni di informatica forense, per maggiori info consultare la pag. web https://www.securfor.it/copia-di-informatica-forense

[101] S. Venturini, *Sequestro probatorio e fornitori di servizi telematici*, dal testo Internet provider di L. Lùparia, Giuffrè 2009.

[102] A livello europeo, esistono delle linee guida per l'identificazione e la gestione delle fonti di prova digitale. Si tratta di norme di soft law che rappresentano la traduzione operativa delle generiche formule adoperate a livello legislativo per garantire l'autenticità della prova digitale nel processo penale.

Si tratta di modelli operativi che la comunità scientifica di riferimento riconosce come il protocollo più corretto per lo svolgimento di una determinata operazione tecnica.
Non esiste una metodologia condivisa per il trattamento delle prove digitali forensi. Vi son una serie di procedure più o meno consolidate.
La giurisprudenza statunitense ha affermato che «*l'investigazione digitale deve essere considerata più un'arte che una scienza*», criticando ogni forma di limitazione alle metodologie investigative in ambito informatico.
Le fasi di cui si compone l'attività investigativa sono:

- Quella "*dell'individuazione"* del reperto informatico d'interesse.

- Quella "*dell'acquisizione".* È la fase che presenta maggiori criticità. Essa consiste in un'operazione di estrapolazione e riproduzione su idoneo supporto del dato digitale oggetto di indagine. Il tutto deve preferibilmente svolgersi nella piena garanzia di integrità e non alterabilità delle tracce, nella prospettiva di una eventuale ripetibilità dell'operazione e tenendo presente la necessità di garantire la genuinità del dato informatico[103]. Dal punto di vista tecnico, l'integrità dei file originali può essere garantita attraverso la c.d. bit stream image, ovvero una copia-clone (bit a bit), on site, delle informazioni digitali. A differenza di un semplice backup dei dati, che si preoccupa di salvare su un supporto differente una copia dei dati presenti sul disco originale, una copia bit a bit è un duplicato esatto dell'intero supporto originale.

- Quella della "*conservazione*" che mira a garantire l'integrità delle prove dalla presenza di fattori esterni che ne alterino il contenuto. Deve essere dedicata massima cura alla catena di custodia, *chain of custody*, ovvero alla metodologia di custodia e di trasporto, sia fisico sia virtuale delle digital evidences.

[103] Aterno S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, Giur. merito, fasc.4, 2013, pag. 0955B.

- Quella di *analisi dei dati e presentazione dei risultati.* L'utilizzo di specifici software consente di estrapolare dal contenuto dei file tutta una serie di informazioni che possono tornare utili ai fini delle strategie processuali delle parti. I risultati raggiunti vengono trascritti in una relazione tecnica: questo documento deve descrivere tutte le operazioni compiute per il raggiungimento del risultato dell'analisi del dato digitale [104].

Tutto ciò è possibile grazie alla collaborazione degli *Internet Service Provider,* società che forniscono connettività ai propri utenti.

Compito della Polizia giudiziaria (PG) è quello di andare alla ricerca, per lo sviluppo delle indagini, di due tipi di dati digitali: quelli che consentono l'identificazione di un potenziale criminale *(Indirizzo IP)* e quelli che ne determinano la sua attività online *(file di log)*.

L'indirizzo IP è un numero che identifica un dispositivo collegato a una rete telematica: esso può essere paragonato a un indirizzo stradale o a un numero telefonico. Il fornitore di connettività dato un indirizzo IP e l'ora di accesso a tale indirizzo, è in grado di fornire i dati personali di chi ha sottoscritto il contratto per usufruire dei servizi di connessione.

Il file di log, invece, è un file in cui sono memorizzate le attività compiute da un determinato utente e consente, pertanto, di ricostruirne i movimenti.

I problemi esposti, unitamente all'incessante sviluppo della tecnologia informatica, hanno aumentato la pressione nei confronti dei sistemi penali nazionali affinché venissero adottati strumenti e procedure uniformi nella gestione dei crimini informatici e dei dati digitali connessi.

Tale prospettiva ha condizionato anche il sistema processuale italiano, nel quale ormai risulta evidente l'importanza esponenziale della prova digitale.

[104] G. Vaciago, *Profili processuali delle indagini informatiche*, in *Diritto dell'internet*, Padova, 2013.

Nell'ordinamento penale italiano non esiste una definizione generale di prova digitale. L'unico riferimento è alla normativa amministrativa, nello specifico all'art. 1, lett. p), del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) che definisce il documento informatico come "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*"[105].

In assenza di definizione, alle *digital evidence* si applica la disciplina delle prove in generale del codice di rito, come modificate dalla legge che autorizza la ratifica della Convenzione di Budapest sulla cybercriminalità.

[105] S. Conti, op. cit. p. 124, pp. 153-164