UNIVERSITÀ DEGLI STUDI
DI MILANO

XXXX

Politecnico di Milano – DATA

Avv. Giulia Escurolle

I Reati informatici

I «**reati informatici**», introdotti per la prima volta nel Codice Penale dalla **L. 547/1993** riguardano tutte quelle condotte illecite commesse mediante l'impiego di tecnologie informatiche o telematiche.

La L. 547/1993 contiene «Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica».

- Prima della legge n. 547 del 1993, nel nostro ordinamento non esisteva alcuna disposizione normativa specifica sui reati informatici.

- A fronte della necessità di approntare un'adeguata tutela giuridica in presenza di nuove forme di aggressione "tecnologica", si era posto il problema dell'applicabilità in via estensiva e, soprattutto, analogica delle norme penali preesistenti. I principi di legalità e tassatività rendevano molto difficoltosa l'applicazione delle norme penali a tali nuove fattispecie criminose.

I Reati informatici

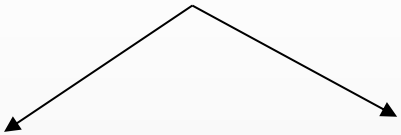
- Il legislatore negli anni ha rilevato che i codici penali dei singoli Paesi non prevedevano le fattispecie necessarie per identificare e perseguire i delitti informatici.

- Le fattispecie relative ai computer crimes venivano quindi ricondotte, con molte difficoltà e forzature, nell'ambito applicativo delle preesistenti norme incriminatrici, come quelle sul furto, sul danneggiamento, sulla frode o sulla truffa.

- Per questo motivo, il Consiglio d'Europa emanò il 13 settembre 1989 la Raccomandazione «**Sur la criminalité en relation avec l'ordinateur**».

I Reati informatici

In questa **Raccomandazione** tutte le possibili fattispecie di abuso dei sistemi informatici e dei dati venivano raggruppate in due gruppi:



Una lista «minima» per la quale gli Stati erano invitati a prevedere una sanzione penale.

Una lista «facoltativa», per la quale la repressione penale era lasciata alla discrezionalità dei singoli Paesi.

I Reati informatici in Italia

- L'Italia, come detto, ha risposto con la Legge 23 dicembre 1993 n. 547 che per la prima volta, ha introdotto una sanzione per qui casi in cui si verifichi un accesso abusivo **ad un computer o ad un sistema software o telematico**, con un aggravamento della pena nei casi in cui dal reato derivi anche il danneggiamento del sistema, o la distruzione dei dati in esso contenuti.

I Reati informatici in Italia

- Viene inoltre attribuita la natura di documento informatico ai supporti di qualunque specie contenenti dati, informazioni o programmi.

- Vengono inserite nuove norme del codice di procedura penale che prevedono la possibilità di effettuare intercettazioni informatiche o telematiche (266-bis c.p.p.).

L’ampiezza del cybercrime

Il campo del cybercrime, tuttavia, ha da sempre avuto la **tendenza ad espandersi** e a ricomprendere anche quei comportamenti criminali riferiti a determinati reati che possono avvenire **anche** con l’ausilio degli strumenti informatici, come ad esempio lo scambio lungo i canali telematici di immagini o video sessualmente espliciti aventi ad oggetto minori oppure quelle forme di violenza che ricadono sotto le categorie del cyberstalking o del cyberbullismo.

Reati informatici in senso stretto

Proprio a causa dell'ampiezza del concetto di cybercrime, la dottrina ha voluto distinguere:

1) i reati informatici **in senso stretto** che possono essere commessi esclusivamente mediante un sistema informatico o telematico oppure sui dati in esso contenuti (ad es. l'accesso abusivo a un sistema informatico o telematico; la detenzione e diffusione abusiva di codici d'accesso a un sistema informatico o telematico; il danneggiamento informatico).

Reati informatici in senso ampio

2) i reati informatici **in senso ampio** nei quali sono ricomprese tutte quelle condotte per le quali lo strumento informatico **costituisce solo un mezzo per la loro commissione agevolata.**

Si tratta di reati che possono essere commessi ***anche*** mediante strumenti informatici o telematici, o su oggetti informatici, per cui

Ad es. reati in materia di diritto d'autore o a danno della proprietà intellettuale per i quali le reti telematiche costituiscono un'agevolazione nella diffusione di opere protette o i reati in materia di pornografia minorile che possono riguardare, oltre a materiale informatico o digitale, anche materiale cartaceo o fotografico.

Un esempio

Recentemente, è stato introdotto nel nostro ordinamento dalla Legge 19 luglio 2019, n. 69 il delitto di cui all'art. **612 ter c.p.** (c.d. revenge porn) che punisce chiunque ceda, pubblichi o diffonda immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate.

Il contesto globale attuale

- La digitalizzazione delle attività lavorative e ludiche rende indispensabile l'utilizzo degli strumenti informatici e telematici.

- Il **livello di esposizione** delle aziende e dei cittadini a **fenomeni di cybercriminalità è pertanto cresciuto esponenzialmente;**

- Le forme di criminalità sono ormai passate dal mondo analogico al **mondo digitale**, specialmente in ambito d'impresa: i dati della propria azienda o dei propri clienti sono ormai, a tutti gli effetti, un asset prezioso da proteggere.

Casi noti recenti

- Nel 2016 a seguito di un attacco informatico vengono sottratti 81 milioni di dollari alla Banca del Bangladesh.
- Nel 2017 il **ransomware WannaCry** si diffonde in tutto il mondo colpendo alcune strutture erogatrici di servizi essenziali, quali il National Health Service inglese.
- Nel 2020 un attacco a FireEye compromette diversi software di sicurezza.

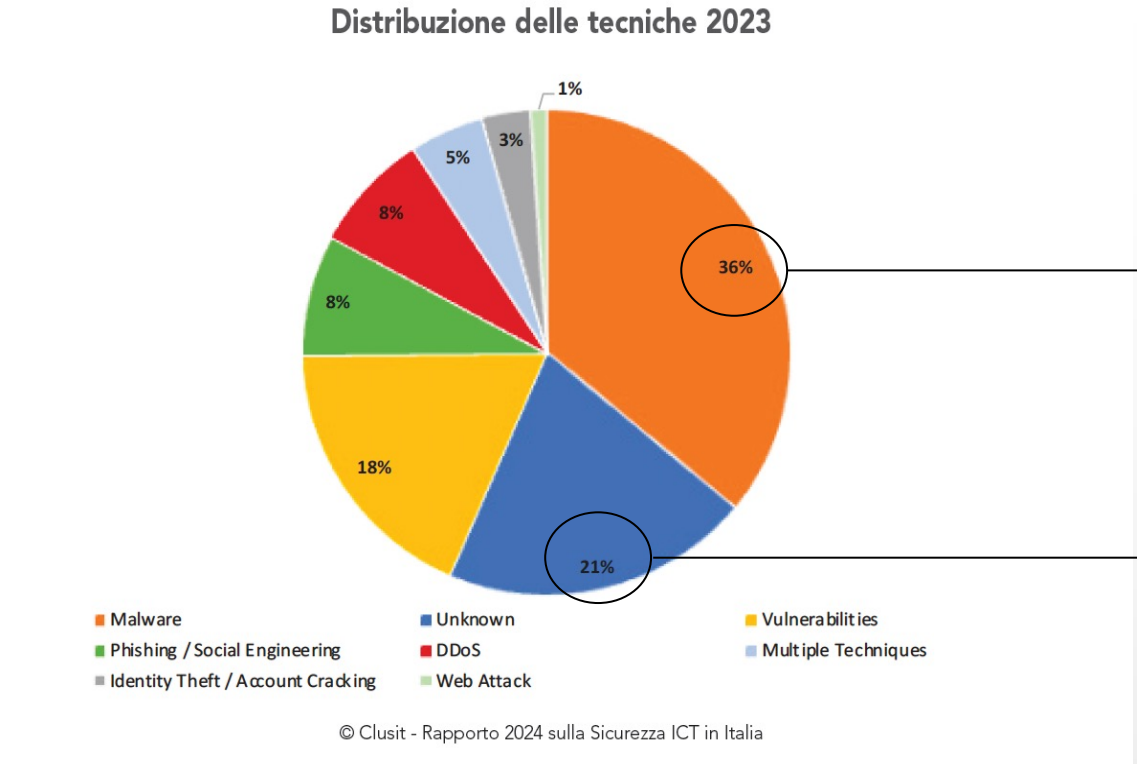
Casi noti recenti

- Nel 2018 la catena di hotel Marriott è stata attaccata, mettendo a rischio i dati di 500 milioni di clienti;
- Nell'estate 2018, un attacco informatico ha colpito la compagnia aerea British Airways a cui sono stati sottratti i dati di quasi 500.000 clienti di (in alcuni casi anche numeri di carta di credito e CVV).

Il rapporto Clusit 2024

- Nella propria relazione sulla sicurezza ICT in Italia, l'**Associazione Italiana per la Sicurezza Informatica (CLUSIT)**, ha evidenziato che nel 2023 si è registrata una crescita del +12% di attacchi rispetto al 2022.

Le tecniche di attacco

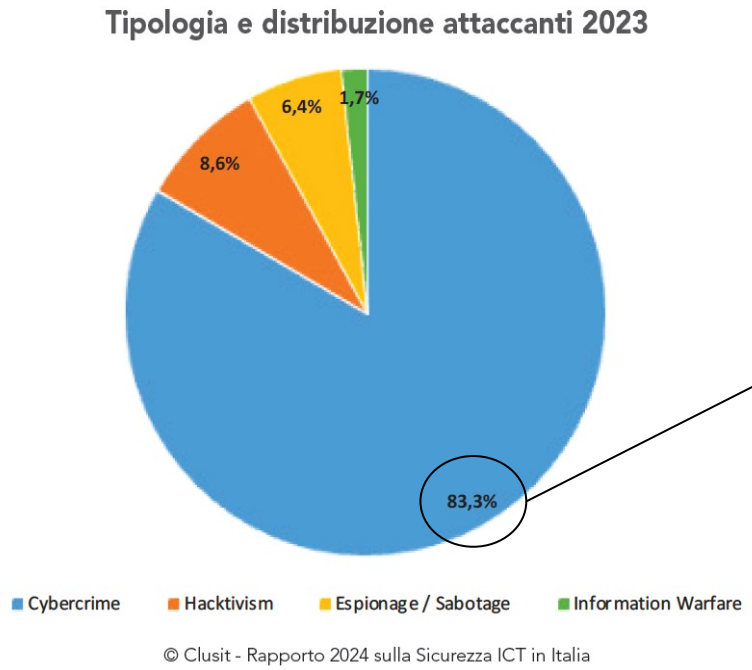


La maggior parte tramite Malware (36%).

Un dato allarmante: il 21% di attacchi sono avvenuti con tecniche non riconosciute.

La tipologia di attacchi

Panoramica sull'evoluzione del cyber crime in Italia e nel mondo - Analisi dei principali cyber attacchi noti del 2023 a livello globale

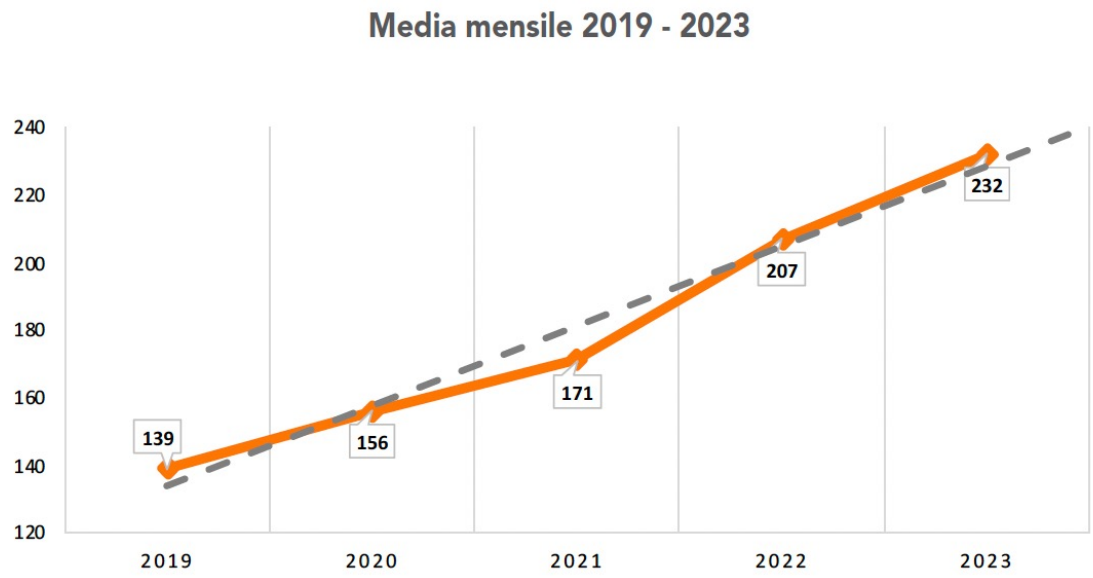


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Quanto alla tipologia di attaccanti, vediamo che nella maggioranza dei casi (83%), si tratta di reati informatici.

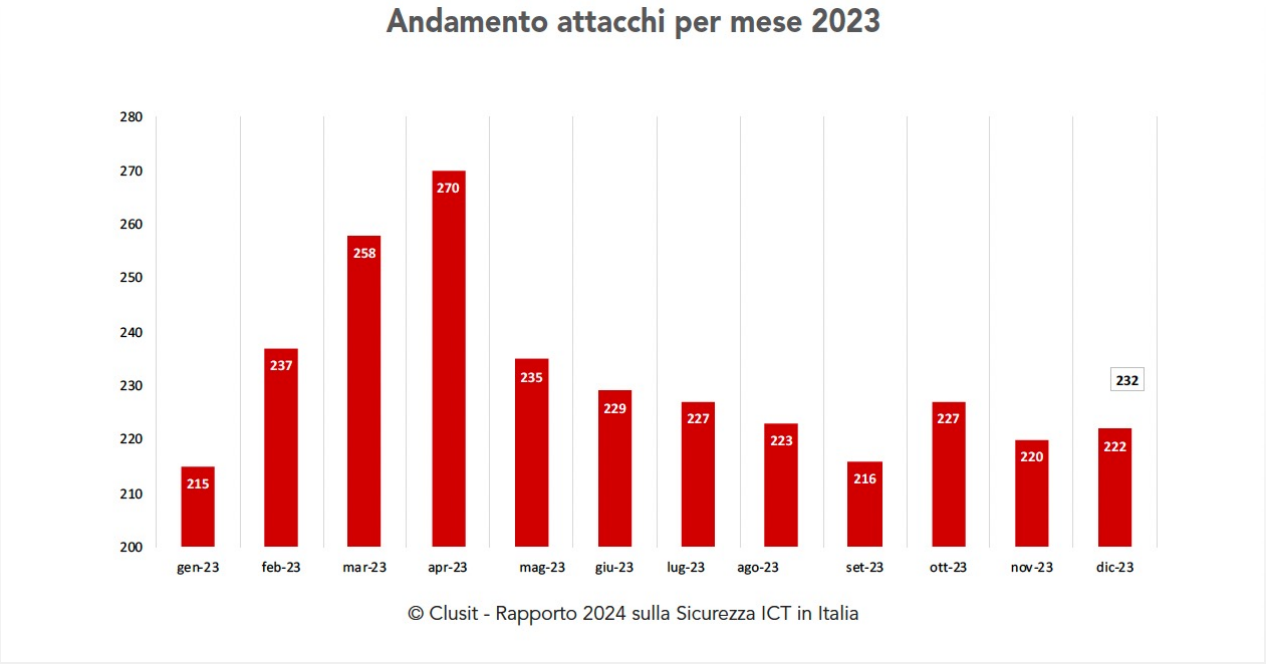
La media mensile di attacchi

Panoramica sull'evoluzione del cyber crime in Italia e nel mondo - Analisi dei principali cyber attacchi noti del 2023 a livello globale



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Gli attacchi nel corso del 2023



La Convenzione di Budapest

- La **Convenzione del Consiglio d'Europa sulla Criminalità informatica** (STE n. 185) è stata sottoscritta a Budapest il 23.11.2001 da **30 paesi**, tra cui l'Italia.

- La Convenzione è stata poi **ratificata da 5 Stati**, per cui è divenuta **esecutiva nel luglio del 2005**.

- Prevede l'introduzione di specifiche norme per contrastare la criminalità informatica.

- È stata adottata nel nostro ordinamento con **la legge 18 marzo 2008, n. 48**.

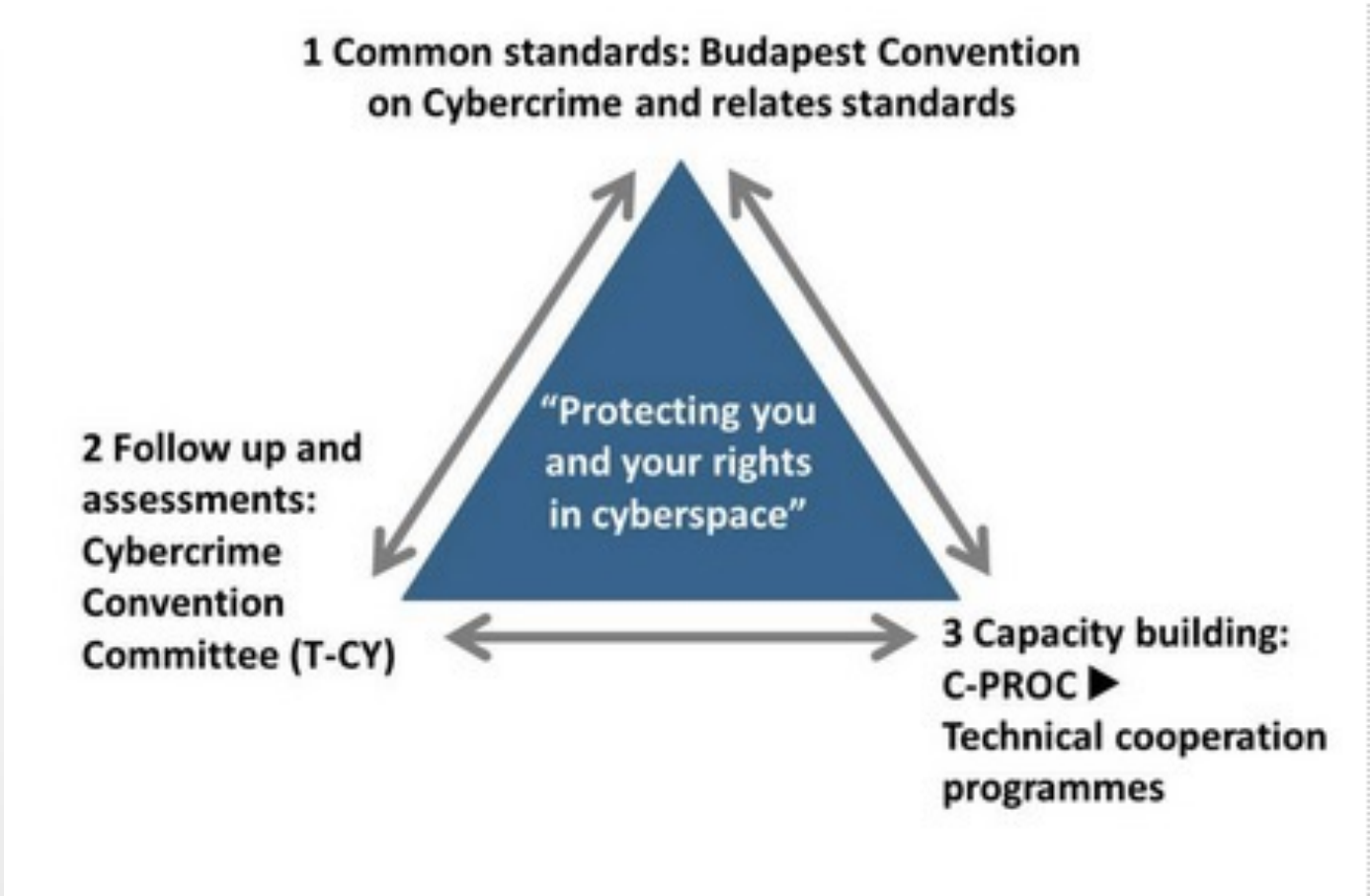
Perchè una Convenzione?

Diversi i motivi e gli obiettivi che hanno condotto alla Convenzione di Budapest.

1. Innanzitutto il carattere trans-nazionale del cosiddetto *cyber crime*, il crimine informatico. Il soggetto che realizza la condotta criminosa generalmente agisce tramite un *personal computer* e, a partire da quel momento, *"l'azione telematica viene realizzata attraverso la connessione fra sistemi informatici distanti fra loro, per cui gli effetti della condotta possono esplicarsi in un luogo diverso da quello in cui l'agente si trova ad operare"*.

- In secondo luogo, si è positivizzato il bisogno di armonizzare i diversi quadri normativi vigenti nei diversi Paesi, nel tentativo di uniformare ed avvicinare il più possibile le legislazioni, gli strumenti applicativi, i controlli e, una parola l'effettività della tutela penale.

Gli strumenti della Convenzione



I numeri della Convenzione

- Ad oggi **66 Paesi hanno firmato e ratificato** il trattato e altri 3 Paesi hanno firmato il trattato ma ancora non l'hanno ratificato nel proprio ordinamento interno.

- Essendo stata proposta dal Consiglio d'Europa, la Convenzione di Budapest non si limita ai soli Paesi europei ma **vi hanno aderito anche nazioni extra-europee** come il Canada, il **Giappone**, **Israele** e gli **Stati Uniti d'America**.

- La Convenzione rappresenta, al momento, l'unico trattato internazionale di contrasto ai crimini informatici.

Gli obiettivi della Convenzione

1) **Armonizzare il diritto penale interno** ai singoli stati prevedendo delle fattispecie di reato comuni e un livello sanzionatorio condiviso per alcune specifiche condotte che rientrano nel cosiddetto cybercrime.

2) **Integrare i codici di procedura penale nazionali** con previsioni che consentano alle forze dell'ordine e alla P.G. di avere i poteri necessari per investigare e perseguire i reati commessi mediante un sistema informatico o che comportino la raccolta ed analisi di evidenze in formato digitale.

Gli obiettivi della Convenzione

3) Predisporre un **insieme di strumenti di cooperazione internazionale** per garantire l'effettiva prosecuzione delle indagini anche qualora le tracce del reato dovessero superare i confini nazionali, cosa molto frequente nei casi di criminalità informatica.

La struttura della Convenzione

- La Convenzione di Budapest è composta da quattro capitoli:

1. Definizioni;
2. Provvedimenti da adottare a livello nazionale;
3. Cooperazione internazionale;
4. Disposizioni finali.

- Il capitolo 2 è diviso in due Sezioni: una dedicata alle previsioni di **diritto penale sostanziale** e una dedicata a quelle di **diritto penale processuale.**

Il diritto penale sostanziale

Per le previsioni di diritto penale sostanziale vengono definite n. **9 fattispecie** di reato suddivise in quattro differenti categorie:

- accesso abusivo;
- intercettazione abusiva;
- danneggiamento di dati;
- danneggiamento di sistemi informatici e telematici;
- utilizzo illecito di apparecchiature e codici d'accesso;
- falsificazione informatica;
- frode informatica;
- reati relativi alla pornografia infantile;
- reati contro la proprietà intellettuale e diritti connessi.

Il diritto penale processuale

Le previsioni di diritto processuale penale, che estendono il loro ambito di applicazione anche oltre le fattispecie previste dalla Convenzione di Budapest, trovano applicazione in ogni reato che sia commesso mediante un sistema informatico o telematico oppure che comprenda il trattamento di una fonte di prova digitale e determinano le condizioni e le tutele che sono applicabili a tutte le indagini.

Il diritto penale processuale

Le condizioni e le tutele sono applicabili anche ad alcune fattispecie ad hoc quali:

- conservazione rapida di dati informatici;
- la conservazione e consegna rapida di dati relativi al traffico;
- l'ingiunzione di produrre dati informatici;
- la perquisizione e sequestro di dati informatici immagazzinati;
- la raccolta in tempo reale di dati sul traffico;
- l'intercettazione di dati relativi al contenuto delle comunicazioni;
- giurisdizione sui crimini transfrontalieri.

I punti di contatto 24/7

La Convenzione di Budapest ha previsto la creazione di una **rete di punti di contatto attiva 24/7** per consentire un'efficace e spedita prosecuzione dell'attività investigativa tra i Paesi membri della Convenzione, anche qualora tale attività debba svolgersi al di fuori dei confini territoriali dell'autorità procedente.

I protocolli

Alla Convenzione di Budapest è anche collegato un Protocollo per il contrasto della xenofobia e del razzismo, qualora materiali, minacce o messaggi con contenuto di odio razziale vengano veicolate lungo i canali telematici ed è attualmente in fase di sottoscrizione un secondo Protocollo sull'attività investigativa nei sistemi di cloud computing.

Le fattispecie in Italia: l'accesso abusivo

L'art. **615-ter c.p.** punisce con la reclusione fino a tre anni «*chiunque abusivamente* ***si introduce*** *in un sistema informatico o telematico protetto da misure di sicurezza ovvero* ***vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo***».

L’accesso abusivo: le aggravanti

La pena è della reclusione da **uno a cinque anni**:

1) se il fatto è commesso da un **pubblico ufficiale** o da un **incaricato di pubblico servizio**, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

L’accesso abusivo: le aggravanti

2) se il colpevole per commettere il fatto usa **violenza sulle cose o alle persone**, ovvero se è palesemente armato;

L’accesso abusivo: le aggravanti

3) se dal fatto **deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento**, ovvero la **distruzione o il danneggiamento dei dati**, delle informazioni o dei programmi in esso contenuti.

L’accesso abusivo: le aggravanti

*«Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da **tre a otto anni**».*

L’accesso abusivo: la procedibilità

- Ipotesi previste dal I comma dell’art. 615-ter → il delitto è punibile a **querela della persona offesa**;

- In tutte le altre ipotesi (aggravate): **si procede d'ufficio**.

- La norma, posta tra i delitti contro la **inviolabilità del domicilio (art. 614 c.p.)** da cui assorbe la stessa funzione sociale e, sostanzialmente, lo stesso trattamento sanzionatorio, prende in considerazione due condotte: quella dell'accesso non autorizzato, rectius abusivo, ad un sistema informatico o telematico, e quella dell'illecito mantenimento.

- La scelta del legislatore di operare questa distinzione appare corretta in quanto esiste la concreta possibilità che **un soggetto acceda, perché autorizzato,** legittimamente all'interno di un sistema ma decida successivamente di trattenersi in maniera abusiva.

- Il mantenimento abusivo si configura anche quando il reo utilizzi il sistema **per finalità diverse, o ulteriori,** rispetto a quelle per cui era stato inizialmente autorizzato l'accesso.

Definizione di Sistema informatico

L'art. 1 della Convenzione di Budapest

«**Sistema informatico**» → 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.

Definizione di Sistema informatico

«**Dati informatici**» → 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;

Definizione di Sistema informatico

«**trasmissione di dati**» → 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.

Definizione di Sistema informatico

«*Proprio in considerazione delle predette caratteristiche, che secondo il Trattato individuano gli elementi essenziali dei crimini informatici,* ***le carte di debito o di credito, identificate da una banda magnetica ovvero da un chip****, elementi entrambi* ***idonei a memorizzare e trasmettere dati informatici****, costituiscono un vero e proprio sistema informatico, capace di elaborare dati, rendendoli operativi, nel momento in cui si connettono all'apparecchiatura POS, consentendo l'accesso autorizzato al sistema informatico finanziario delle Banche*»

(Cassazione Pen., sez. Feriale, 12 novembre 2012, n. 43755).

Definizione di Domicilio informatico

*«…con il riferimento al «**domicilio informatico**», sembra che il legislatore abbia voluto individuare il **luogo fisico - come sito in cui si può estrinsecarsi la personalità umana nel quale è contenuto l'oggetto della tutela** (qualsiasi tipo di dato e non i dati aventi ad oggetto particolari contenuti), per salvaguardarlo da qualsiasi tipo di intrusione (ius exludendi alios), indipendentemente dallo scopo che si propone l'autore dell'abuso»*

(Cass. Pen. Sez. VI,.14 dicembre 1999, n. 3067).

Misure di sicurezza

- Altro elemento che caratterizza il reato è rappresentato dalle “misure di sicurezza”.
- L’accesso, infatti, affinché rientri nella previsione del reato deve essere compiuto **violando le misure difensive** poste dal titolare a difesa del sistema.
- La giurisprudenza e la dottrina, infatti, ritengono che la fattispecie in esame non richieda una particolare efficacia delle misure di sicurezza adottate a salvaguardia del sistema, ma è necessaria la **volontà del titolare di reprimere qualsiasi irruzione con accorgimenti tecnici, informatici e logici, anche se facilmente aggirabili** = ne consegue che il reato si perfeziona anche se viene violata una sola misura di sicurezza, non rilevando né il numero né, tantomeno, l’efficacia delle difese adottate dal titolare.

Misure di sicurezza

- Dal punto di vista prettamente tecnico, le misure di sicurezza possono essere divise in due grandi categorie: **misure di sicurezza digitali e misure di sicurezza non digitali**. Le prime si suddividono a loro volta tra quelle software (password, firewall) ed hardware (firma digitale o riconoscimento biometrico). Le seconde vengono utilizzate per proteggere il sistema informatico o telematico con riguardo alla loro materialità (cassaforte, armadietto).

Definizione di Misura di sicurezza

«… deve ritenersi che, ai fini della configurabilità del delitto, assuma rilevanza ***qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso al sistema informatico****, anche quando si tratti di strumenti esterni al sistema e meramente organizzativi, in quanto destinati a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi»*

(Cass. Pen., Sez. V, 6 dicembre 2000, n. 12732).

Definizione di Misura di sicurezza

Ne consegue che «… *perché sussista il crimine ex art. 615-ter* ***è necessario che il sistema informatico o telematico sia protetto da misure di sicurezza che qualcuno abbia neutralizzato***».

(Cass. Pen., Sez. V, 15 febbraio 2007, n. 6459).

Caratteristiche dell'accesso abusivo ad un sistema informatico o telematico

- **Reato comune**

- **Elemento soggettivo** richiesto è il **dolo generico**,ovvero il soggetto agente deve avere la coscienza e la volontà di accedere ad un sistema informatico o telematico provvisto di misure di sicurezza, a nulla rilevando sia il muovente che le finalità del reo.

L’accesso abusivo: l’elemento soggettivo

«Integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter c.p., la condotta di accesso o di mantenimento nel sistema posta in essere da ***un soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare*** *del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che hanno soggettivamente motivato l'ingresso al sistema» .*

(Cass. Pen., SS.UU, 7 febbraio 2012, n. 4694).

L’accesso abusivo: l’elemento soggettivo

*«Integra il delitto previsto dall’ art. 615 ter c.p., comma 2, n. 1, la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, **pur essendo abilitato** e **pur non violando le prescrizioni formali impartite dal titolare** di un sistema informatico o telematico protetto per delimitarne l'accesso, **acceda o si mantenga nel sistema per ragioni ontologicamente estranee** rispetto a quelle per le quali la facoltà di accesso gli è attribuita».*

(Cass. Pen., sez. V, 27 febbraio 2019, n. 8541).

L’accesso abusivo: l’elemento soggettivo

Pertanto, il reato punito dall’art. 615-ter del Codice penale si configura quale **reato di pericolo** che si realizza «*ogniqualvolta l’ingresso abusivo riguardi un sistema informatico in cui sono contenute notizie riservate, **indipendentemente dal tipo di notizia eventualmente appresa***».

(Cass. Pen., sez. V, 27 febbraio 2019, n. 8541; Cass. Pen., 09 novembre 2018, n. 8541).

L’accesso abusivo: il locus commissi delicti

«*l'ingresso o l'introduzione abusiva (…) vengono ad essere* ***integrati nel luogo in cui l'operatore materialmente digita la password*** *di accesso o esegue la procedura di login,* ***che determina il superamento delle misure di sicurezza*** *apposte dal titolare dei sistema, in tal modo realizzando l'accesso alla banca dati*».

(Cass. Pen., Sez. I, 08 settembre 2015, n. 36338).

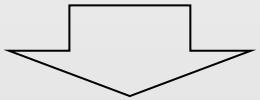
L’accesso abusivo: il locus commissi delicti

*«… da tale impostazione, coerente con la realtà di una rete telematica, **consegue che il luogo dei commesso reato si identifica con quello nel quale dalla postazione remota l'agente si interfaccia con l'intero sistema**, digita le credenziali di autenticazione e preme il tasto di avvio, ponendo così in essere l'unica azione materiale e volontaria che lo pone in condizione di entrare nel dominio delle informazioni che vengono visionate direttamente all'interno della postazione periferica».*

(Cass. Pen., Sez. I, 08 settembre 2015, n. 36338).

Accesso abusivo e violazione della corrispondenza

«Integra il reato di cui all'articolo 615-ter del Cp, la condotta di colui che accede abusivamente all'altrui casella di posta elettronica, trattandosi di uno spazio di memoria, protetto da una password personalizzata, di un sistema informatico destinato alla memorizzazione di messaggi, o di informazioni di altra natura, nell'esclusiva disponibilità del suo titolare, identificato da un account registrato presso il provider del servizio».



Accesso abusivo e violazione della corrispondenza

«(…) e in ipotesi di accesso abusivo a una casella di posta elettronica protetta da password, il reato di cui articolo 615-ter del Cp concorre con il delitto di violazione di corrispondenza e con il reato di danneggiamento di dati informatici, nel caso in cui, all'abusiva modificazione delle credenziali d'accesso, consegue l'inutilizzabilità della casella di posta da parte del titolare».

(Cass. Pen., Sez. V, 25 marzo 2019, n. 18284).

Accesso abusivo: accesso a «Dropbox»

«*In tema di accesso abusivo ad un sistema informatico o telematico, la fattispecie di cui l'art. 615-ter, comma primo, cod. pen., contestata in relazione allo spazio di archiviazione c.d. "Dropbox", **postula che sia individuato il soggetto titolare dello spazio e del relativo "ius excludendi alios" all'accesso al suddetto applicativo***»

(Cass. Pen., Sez. V, 22 febbraio 2023, n. 27900).

Accesso abusivo: la revoca dell'accesso

*«Integra il delitto di accesso abusivo ad un sistema informatico la condotta di colui che si introduca, mediante uso di «**password**» **modificate** e contro la volontà del titolare, nel c.d. «**cassetto fiscale**» altrui, spazio virtuale del sistema informatico dell'Agenzia delle entrate di pertinenza esclusiva del contribuente, riconducibile alla nozione di domicilio informatico».*

In motivazione, la Corte ha precisato che **non rileva la pregressa autorizzazione all'accesso rilasciata dal titolare per vincolo familiare o affettivo e poi revocata mediante comportamenti concludenti!**

(Cass. Pen., Sez. V, 15 febbraio 2021, n. 15899).

Accesso abusivo: la qualifica dell'autore

«in tema di accesso abusivo a un sistema informatico, ai fini dell'integrazione della circostanza aggravante di ***abuso della qualità di operatore del sistema****, riveste siffatta qualifica non solo il titolare di poteri decisori sulla gestione dei contenuti o sulla configurazione del sistema, ma* ***anche colui che, pur se destinato a svolgere compiti meramente esecutivi****, sia comunque abilitato a operare sul sistema, modificandone i contenuti o la struttura»*.

(Cass. pen., sez. V, 24 gennaio 2022, n.7775).

UNIVERSITÀ DEGLI STUDI
DI MILANO

Grazie per l'attenzione!

giulia.escurolle@unimi.it
g.escurolle@gmail.com