I Reati Informatici

Dott. M. Montulli
Dott. P. Prandini

Definizione:

“Qualsiasi atto o fatto contrario alle norme penali nel quale il computer viene coinvolto come oggetto del fatto, come strumento o come simbolo”

Raccomandazione n. R(89) 9 del 1989

Legge 23 dicembre 1993, n. 547 "*Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*"

- *Lista minima:* frode, il falso di un documento informatico, il danneggiamento e il sabotaggio di dati, gli accessi abusivi a sistemi informatici e la riproduzione non autorizzata di programmi

- *Lista facoltativa:* divulgazione non autorizzata di informazioni, l'uso non autorizzato di programmi, elaboratori o reti o ancora l'alterazione di dati e programmi quando non costituiscono danneggiamento

Convenzione Internazionale sul Cybercrime, Budapest 23 novembre 2001

Nel rispetto dei diritti umani fondamentali, gli Stati firmatari si impegnano a collaborare per condurre una lotta comune alla criminalità informatica.

Gli obiettivi sono appunto quelli di favorire tale collaborazione e rendere le legislazioni dei Paesi aderenti più simili tra loro, favorendo l'uso di strumenti pratici nelle indagini sui reati informatici

Legge 18 marzo 2008, n. 48: "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*"

Art. 24-bis d.lgs. n. 231/2001 titolato “Delitti informatici e trattamento illecito dei dati”, che prevede che l’ente possa rispondere dei reati informatici compiuti da figure apicali o da dipendenti dell’ente nell’interesse e a vantaggio dell’ente stesso

Comma 1-bis all’art. 247 c.p.p. in tema di conservazione dei dati originali, di perquisizione di un sistema informatico o telematico che si presuma contenere dati, informazioni o programmi o tracce pertinenti al reato, anche se protetto da misure di sicurezza, il quale impone di adottare tecniche che ne assicurino la conservazione e ne impediscano l’alterazione

Comma 1 dell’art. 254 c.p.p., il quale ricomprende nelle ipotesi di sequestro anche la corrispondenza inoltrata per via telematica quando abbia a che fare con l’imputato di un procedimento o possa avere relazione con il reato

Art. 254-bis che disciplina il sequestro di dati informatici presso fornitori di servizi informatici, telematici o di telecomunicazioni

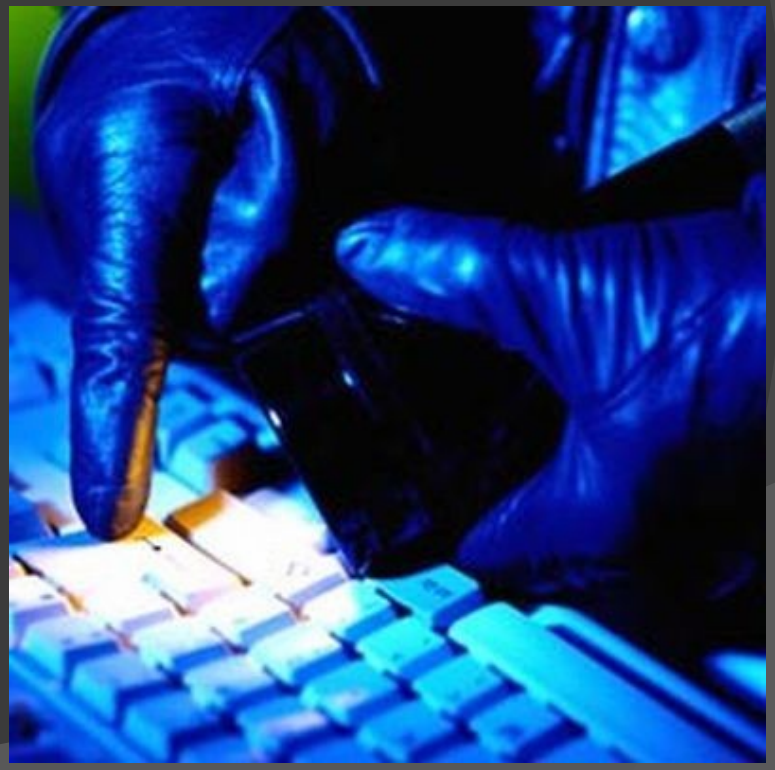
Artt. 256, 259 e 260 c.p.p. finalizzati a disciplinare l’acquisizione dei dati informatici da utilizzare come elementi di prova

Artt. 352, 353 e 354 c.p.p. che stabiliscono l’adozione di misure tecniche da parte degli ufficiali di polizia giudiziaria nell’acquisizione degli elementi probatori al fine di consentire la conservazione e l’inalterabilità di dati, informazioni, programmi e sistemi informatici

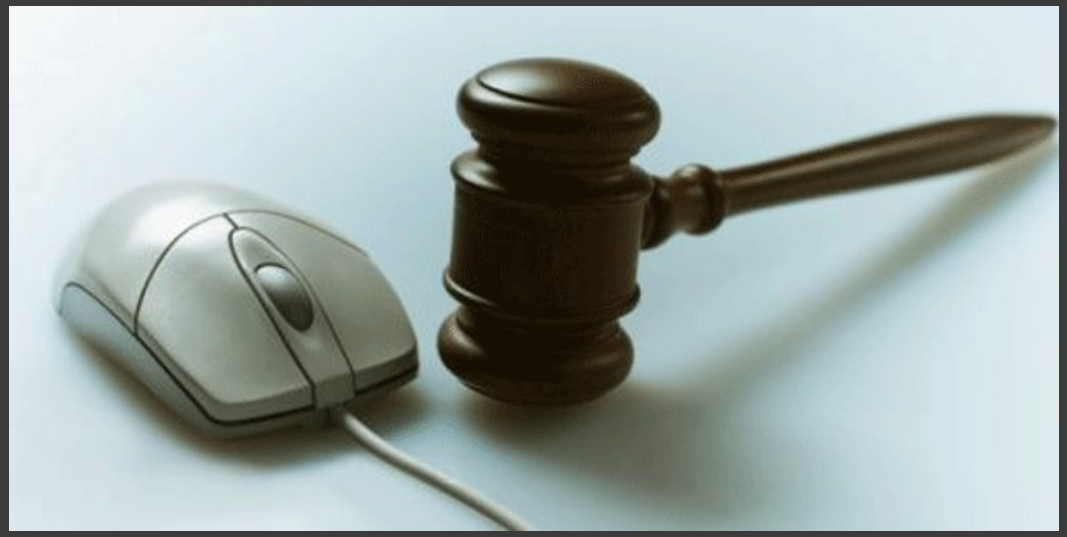
CODICE DELLA PRIVACY:

L’art. 10 della legge n. 48/2008 introduce una modifica all’art. 132 del codice stabilendo che Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza e gli altri soggetti di cui al comma 1 dell’art. 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, anche quando lo richiedano autorità investigative straniere, possono ordinare ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere per un termine di novanta giorni, prorogabili a sei mesi, i dati relativi al traffico telematico quando ciò sia necessario per l’accertamento e la repressione di alcuni reati o per esigenze investigative.

La norma stabilisce altresì che entro 48 ore il pubblico ministero del luogo di esecuzione, ravvisata la ricorrenza dei motivi, convalida il c.d. “CONGELAMENTO DEI DATI” (in mancanza di convalida l’ordine decade) e impone comunque che il fornitore o l’operatore mantenga il segreto sull’ordine di conservazione ricevuto



Art. 51 c.p.p., ultimo comma, che stabilisce che per i reati tentati o consumati, relativi alla pornografia minorile, all'accesso abusivo, alla corrispondenza, alle intercettazioni, al danneggiamento di sistemi e dati informatici e al reato di frode informatica, le indagini sono affidate al pubblico ministero presso il tribunale del capoluogo di corte d'appello.



Con tale previsione sembra evidente l'intenzione del legislatore di voler favorire la nascita di una categoria di magistrati che, attraverso corsi di formazione periodica, con l'ausilio di consulenti tecnici esperti di informatica, acquisiscano una sorta di specializzazione nella conduzione delle indagini relative ai reati di cui l'articolo fa menzione

- Art. 491-bis c.p.: il falso informatico e l'estensione al reato delle disposizioni sulla "falsità in atti"
- Art. 495-bis c.p.: falsità rese al certificatore di firme digitali
- Art. 615-ter c.p.: la tutela del domicilio informatico
- Art. 615-quater c.p.: detenzione e diffusione abusiva di codici d'accesso
- Art. 615-quinquies c.p.: diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o telematico
- Art. 616 c.p.: violazione, sottrazione e soppressione di corrispondenza

intercettazione, interruzione, falsificazione e soppressione di comunicazioni informatiche o telematiche

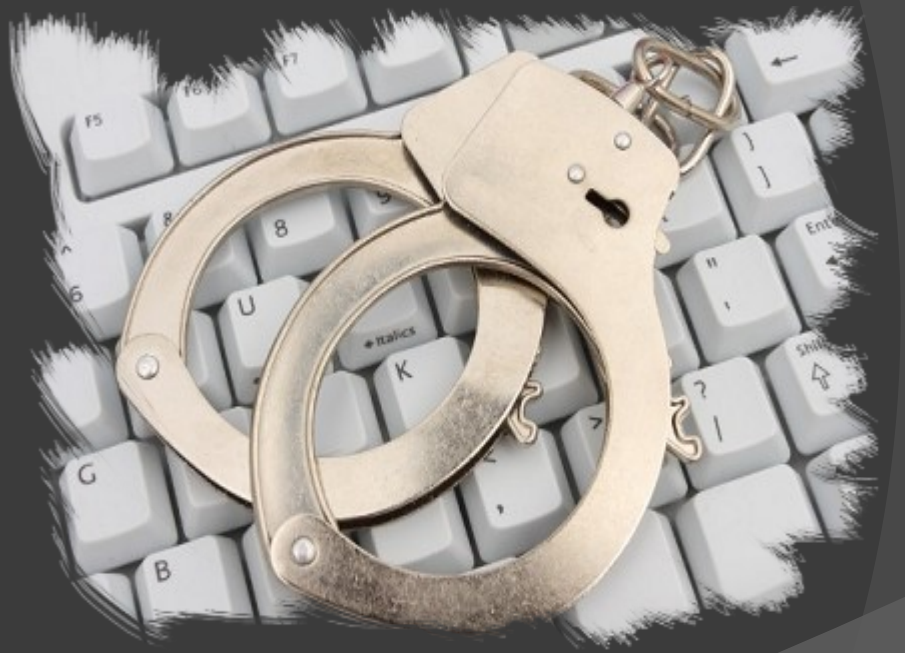
- ✓ Art. 617-quater c.p.
- ✓ Art. 617-quinquies c.p.
- ✓ Art. 617-sexies c.p.

danneggiamento di dati, programmi, informazioni e sistemi informatici

- Art. 635-bis c.p.
- Art. 635-ter c.p.
- Art. 635-quater c.p.
- Art. 635-quinquies c.p.

La tutela penale del diritto d’autore

- Art. 171 LDA
- Art. 171-bis LDA
- Art. 171-ter LDA
- Art. 171-quater LDA
- Art. 171-octies LDA



L’art. 640-ter c.p.:
LA FRODE INFORMATICA

PHISHING (da to fish = pescare), un reato il cui primo obiettivo è carpire username e password altrui al fine di utilizzarli per accedere al conto corrente online dell’utente e distrarne, a proprio o altrui vantaggio, somme di denaro avendo cura di non lasciare traccia dei movimenti

VISHING (vocal phishing che sfrutta la tecnologia VoIP – voice over IP) che nel simulare una chiamata come proveniente da un call center autorizzato, induce l’utente a comunicare dati che possono essere fraudolentemente usati per ottenere vantaggi economici.

SKIMMING Comma 9 dell’art. 55 del d.lgs. n. 231/2007

Polizia Postale e delle Comunicazioni

20 compartimenti, con competenza regionale, e le 80 sezioni con competenza provinciale coordinati dal Servizio Polizia delle Comunicazioni

NOPT: Nucleo Operativo di Polizia delle Telecomunicazioni