

Normativa



Massimo Carnevali

Il materiale di questo corso è distribuito con licenza Creative Commons 4.0 Internazionale: Attribuzione-Condividi allo stesso modo.

<https://creativecommons.org/licenses/by-sa/4.0/>

Dove note sono state citate le fonti delle immagini utilizzate, per le immagini di cui non si è riusciti a risalire alla fonte sono a disposizione per ogni segnalazione e regolarizzazione del caso.

Massimo Carnevali

posta@massimocarnevali.com

<https://it.linkedin.com/in/massimocarnevali>

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Normativa

- Cenni sulla normativa vigente
- Il GDPR

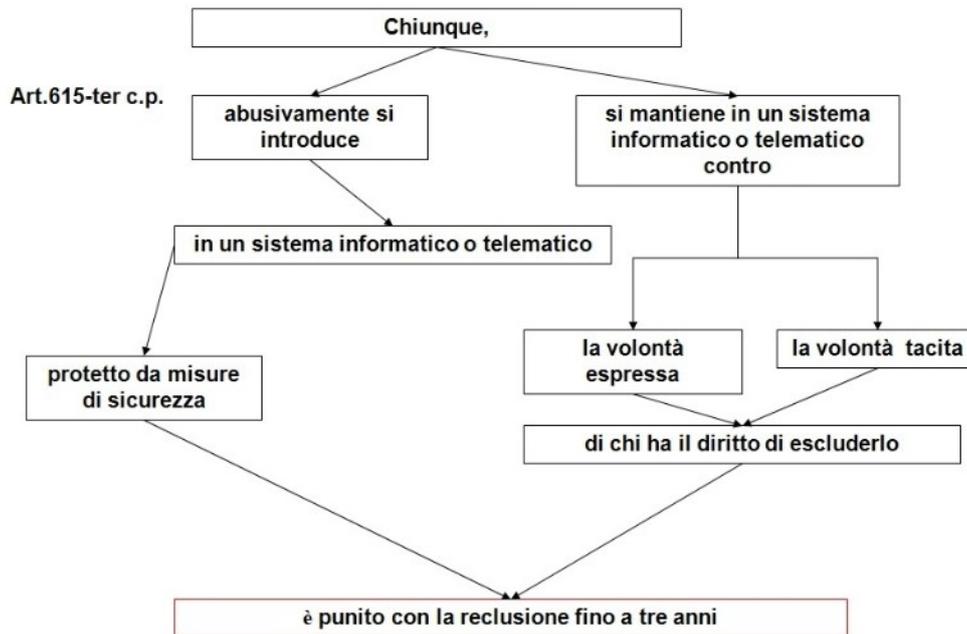
..

Cenni sulla normativa vigente

Cenni (molto vaghi) sulla normativa vigente

Da ingegneri non da avvocati

Cenni sulla normativa vigente



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

4

Codice penale 615 ter (accesso abusivo) da 1 a 3 anni
Procedibile d'ufficio per la pubblica utilità (PA, banche, gestori telefonici, sanità ecc.) altrimenti richiede querela di parte entro 3 mesi da quando te ne sei accorto.

Prescrizione dai 6 ai 10 anni.

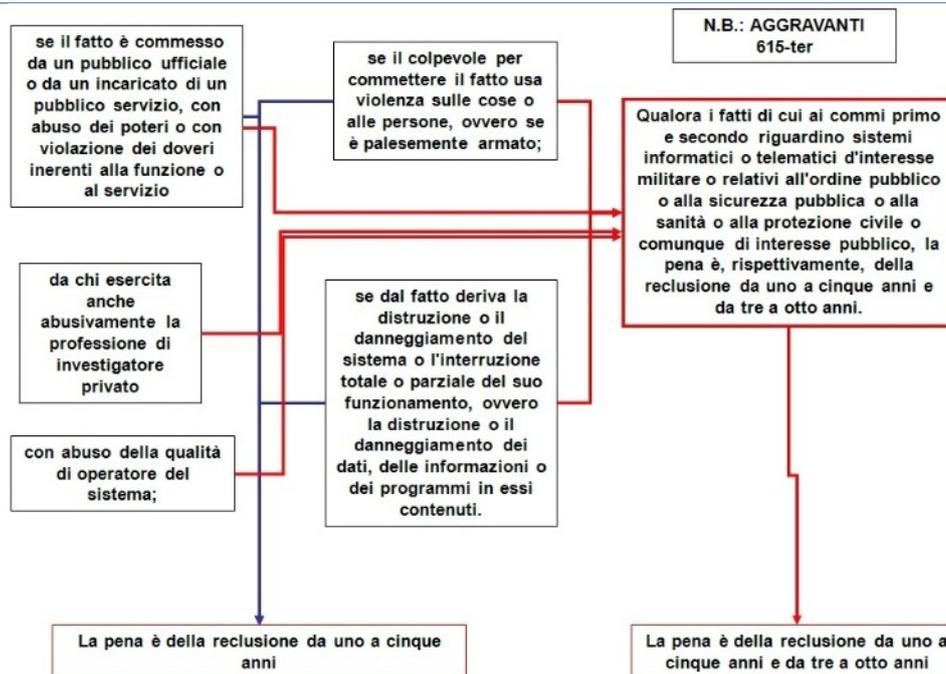
c.p 615 ter (accesso abusivo, ti ho bucato)

c.p 615 quater (ho le credenziali e le ho usate, la sola detenzione non autorizzata non basta, serve l'intento di usarle prima o poi)

c.p 615 quinquies (creazione e diffusione malware a scopo di danno o profitto)

Se cedo le password a qualcuno che poi le usa è favoreggiamento.

Cenni sulla normativa vigente



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

5

Altro articolo correlato: codice penale 635 (danneggiamento informatico).

Cancellazione, deterioramento dati ecc. anche DDOS

Non è necessario che il danneggiamento ci sia, basta l'atto di cercare di farlo (es il mio antivirus ti blocca ma tu sei punibile lo stesso perché ci hai provato)

Vale il nuovo concetto di domicilio informatico (mia mail, mio facebook, mia cloud, tutto ciò che non è pubblico, condiviso solo fra amici).

https://www.youtube.com/watch?v=OzsD_PIG2aA

Cenni sulla normativa vigente

Tutti:

- Normativa per gli Amministratori di Sistema
- GDPR (General Data Protection Regulation (679/2016))
- Responsabilità amministrative degli enti D.Lgs. 231/2001
- Sicurezza sul lavoro (es. operatori VDT) D.Lgs. 81/2008
- Antiriciclaggio e reati finanziari D.Lgs. 231/2007
- Normativa sul diritto d'autore D.Lgs 633/1941 (!?)

Società quotate in borsa:

- Legge 262 (falsa informativa)
- Codice PREDA (danno reputazionale e impatto sul titolo)
- Regolamenti CONSOB

Settori specifici:

- Normative specifiche sui brevetti
- Normative sulla tracciabilità (GDO, alimentari, farmaceutici)
- Infrastrutture critiche
- Carte di credito e dati bancari

NON sono un giurista per cui il livello di dettaglio e il linguaggio sono da ingegneri!

Cenni sulla normativa vigente

Normative per gli **Amministratori di Sistema**

- Identificazione e nomina degli amministratori di sistema
- Valutazione delle caratteristiche personali
- Diverso profilo giuridico
- Tenuta dei log delle operazioni svolte (inalterabile)
- Accesso nominale e non generico (NO root, admin ecc.)
- Problema in caso di servizi in outsourcing, insourcing, cloud ecc.

Testo:

<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499>

il GDPR non prevede una disciplina ad hoc in merito, di conseguenza le prescrizioni del Garante, si assumono tuttora valide.

Cenni sulla normativa vigente

Normativa sul diritto d'autore



D.Lgs. 633/1941 - Art. 96 Il ritratto di una persona non può essere esposto senza il consenso di questa + Art. 595 c.p. "diffamazione"

=

Reclusione da 6 mesi a 3 anni, multa non inferiore a 516€

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

8

https://it.wikipedia.org/wiki/Diritto_d'autore_italiano

Dà della Milf a collega su Facebook: è giusta causa di licenziamento:

<http://www.altalex.com/documents/news/2015/02/19/da-della-milf-a-collega-su-facebook-e-giusta-causa-di-licenziamento>

Dare della Ninfomane alla propria "ex" su Facebook costa: <http://www.comellini.it/H1.htm>

Parere della cassazione sui reati a mezzo Facebook
http://www.corrierecomunicazioni.it/ict-law/27313_diffamazione-massime-la-cassazione-ha-dissipato-il-mistero-su-facebook.htm

Anzi è diffamazione aggravata vista la potenziale estensione della platea del messaggio: Cassazione penale Sezione V, 23/01/2017, n. 8482

In Svizzera Facebook Like a post antisemita è reato
<https://www.bloomberg.com/news/articles/2020-02-20/facebook-likes-of-anti-semitic-posts-may-be-a-swiss-crime>

Cenni sulla normativa vigente

Normativa sul diritto d'autore

- I software ma a volte anche le banche dati o i risultati prodotti dagli stessi software (si compera un supporto e una licenza d'uso non "il software")
- Materiale audio, video, letterario protetto da diritto d'autore
- Verifica dei nomi a dominio, dei marchi, dei loghi
- Utilizzo materiale di terzi protetto da licenza

Due vie di uscita (da usare quando possibile)

Descrizione:

https://it.wikipedia.org/wiki/Diritto_d'autore_italiano

Non è una idea recente: Lo Statuto di Anna è stata la prima legge sul copyright in Gran Bretagna. È stato promulgato nel 1709 ed è entrato in vigore il 10 aprile 1710. E' generalmente considerato il primo statuto completo sul copyright. Prende nome dalla regina Anna, durante il cui regno fu promulgato; oggi è considerato l'origine della legge sul copyright.

https://it.wikipedia.org/wiki/Statuto_di_Anna

Cenni sulla normativa vigente

Software Open Source

- “software distribuito con una licenza che ne consente la libera distribuzione in forma sorgente, e conferisce la possibilità all’utente di poter modificare il programma originario e di poter distribuire la versione modificata”
- Varie licenze, più famosa GPL
- “free speach, not free beer !”
- Le quattro libertà fondamentali del “Free software” sono:
 - 0) La libertà di eseguire il programma
 - 1) La libertà di studiare il programma, e adattarlo alle proprie necessità
 - 2) La libertà di distribuire copie
 - 3) La libertà di migliorare il programma e di rilasciare i propri miglioramenti al pubblico

https://en.wikipedia.org/wiki/Open-source_software

Cenni sulla normativa vigente

Creative Commons



Attribuzione (BY)

Bisogna sempre indicare l'autore dell'opera (attributo obbligatorio) in modo che sia possibile attribuirne la paternità.



Uso non commerciale (NC)

Non sono consentiti usi commerciali dell'opera creativa.



Nessuna opera derivata (ND)

Non sono consentite elaborazioni dell'opera creativa.



Condividi allo stesso modo (SA)

Si può modificare l'opera ma l'opera modificata deve essere rilasciata secondo le stesse condizioni scelte dall'autore originale.



<http://www.creativecommons.it/>

II GDPR

Regolamento **2016/679 EU Data Protection GDPR**
(**General Data Protection Regulation**)

+

Legge italiana 101/18

DECRETO LEGISLATIVO 10 agosto 2018, n. 101

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, **relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

<https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg>

II GDPR

COSA fare
non
COME farlo

Uno dei principi base che la differenziano da altre normative precedenti è il fatto che dice alle aziende **COSA** debbono fare, non **COME** debbono farlo. Misure ADEGUATE, non dice quali ma tu devi valutare quali sono quelle adeguate in relazione alla tecnologia corrente, al rischio dei tuoi dati ecc.

II GDPR

Titolare del trattamento (Data controller)

Titolare del trattamento (Data controller nella versione inglese del testo).

Il titolare del trattamento è responsabile direttamente e personalmente dei trattamenti che avvengono in azienda o nell'ente.

E' possibile un sistema di contitolarità con definizione di ambiti di responsabilità e dei compiti.

Tendenzialmente il legale rappresentante dell'azienda.

Responsabile del trattamento (Data Processor)

Responsabile del trattamento (Data Processor nella versione inglese del testo).

Colui che tratta i dati (su incarico del titolare).

Interno o esterno, deve esserci incarico esplicito formalizzato e deve essere formato per lo scopo.

La responsabilità massima in termini di infrazioni

rimane al titolare del trattamento ma esiste un

concetto di responsabilità solidale fra titolare e

responsabile. Nel caso un trattamento coinvolga più responsabili ovviamente si estende a tutti i

contitolari.

Ha la responsabilità giuridica dei suoi trattamenti.

II GDPR

Dati personali (anche potenzialmente)

Cosa si intende per "Dati personali"? Ovviamente lo sono nome, cognome numero di telefono, email, data e luogo di nascita ecc.

Il concetto di dato personale viene però esteso anche ai dati che "potenzialmente" possono identificare la persona (anche in congiunzione con altri dati). Qualche esempio?

Indirizzi IP, Cookies, RFID, MAC address e codici IMEI possono contribuire a costruire l'identità della persona per cui sono da considerarsi potenzialmente dati personali.

Nessuna distinzione fra dati personali dell'individuo di tipo lavorativo, pubblico o privato.

Dati particolari/speciali ~ "dati sensibili"

All'articolo 9 viene introdotto il concetto di dato particolare o dato speciale, sono particolari dati personali che più o meno corrispondono all'attuale "dato sensibile". Sono dati personali speciali le informazioni relative a razza, etnia, idee politiche, religione, filosofia, iscrizione ai sindacati, stato di salute, inclinazioni sessuali + nuove categorie di dati più "moderni" come quelli genetici, biometrici ecc. I dati speciali possono essere trattati solo con un consenso specifico, e solamente se è necessario per l'esecuzione del contratto. Attenzione perché i diritti dell'interessato decadono se il soggetto ha resi pubblici questi dati spontaneamente (se ad esempio ha deciso di rappresentare in pubblico un partito o un sindacato e ha quindi dichiarato la sua appartenenza).

Violazioni dei dati

Data Breach

“Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

72 ore, tempo entro cui le violazioni di sicurezza o le perdite di dati personali dovranno essere segnalati all'autorità di controllo e, nel caso impatti i loro diritti, anche agli interessati.

II GDPR

Altri elementi

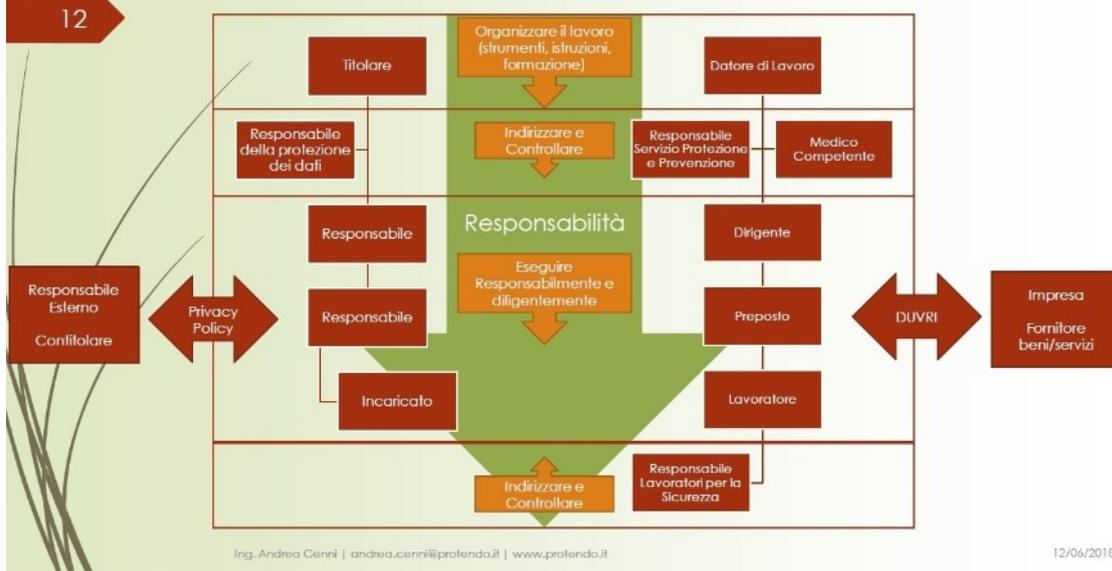
- Deroghe per aziende sotto i 250 dipendenti (semplificazione)
- Consenso e informativa
- Responsabile della protezione dei dati (Data protection officer)
- Registro dei trattamenti. Analisi dei rischi ed elenco trattamenti

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Altri elementi

II GDPR

1.5 Convergenza tra Security (GDPR) e Safety (D.lgs. 81/08) – Albero delle responsabilità



.....