# Corso di Formazione Manageriale

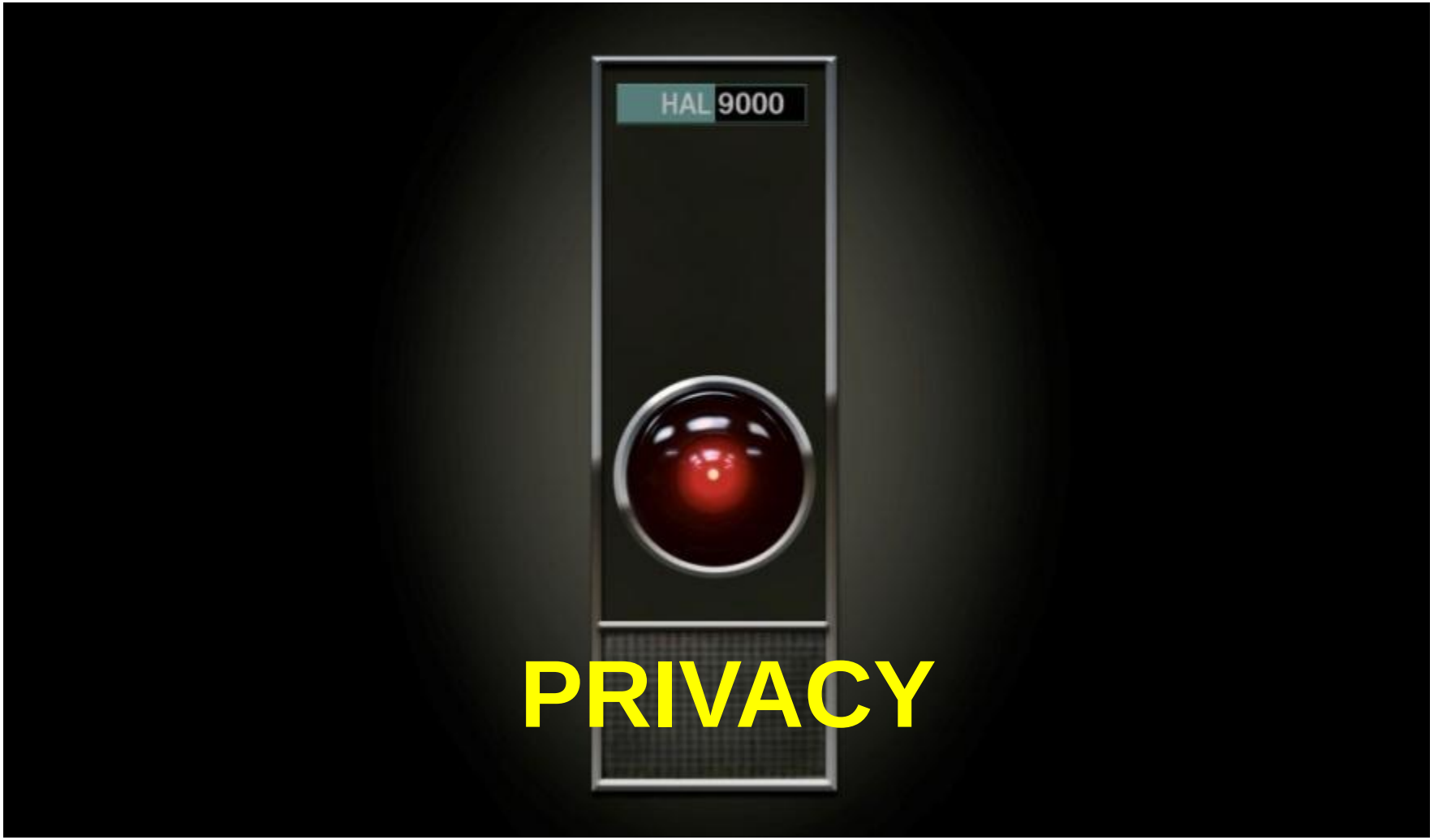
# Responsabile protezione dei dati "DPO" UE 2016/679

## *Modulo 4 – Sicurezza Informatica e Reati Informatici*

# *M4.1* – Sicurezza del trattamento dati

## *Il concetto di Privacy*

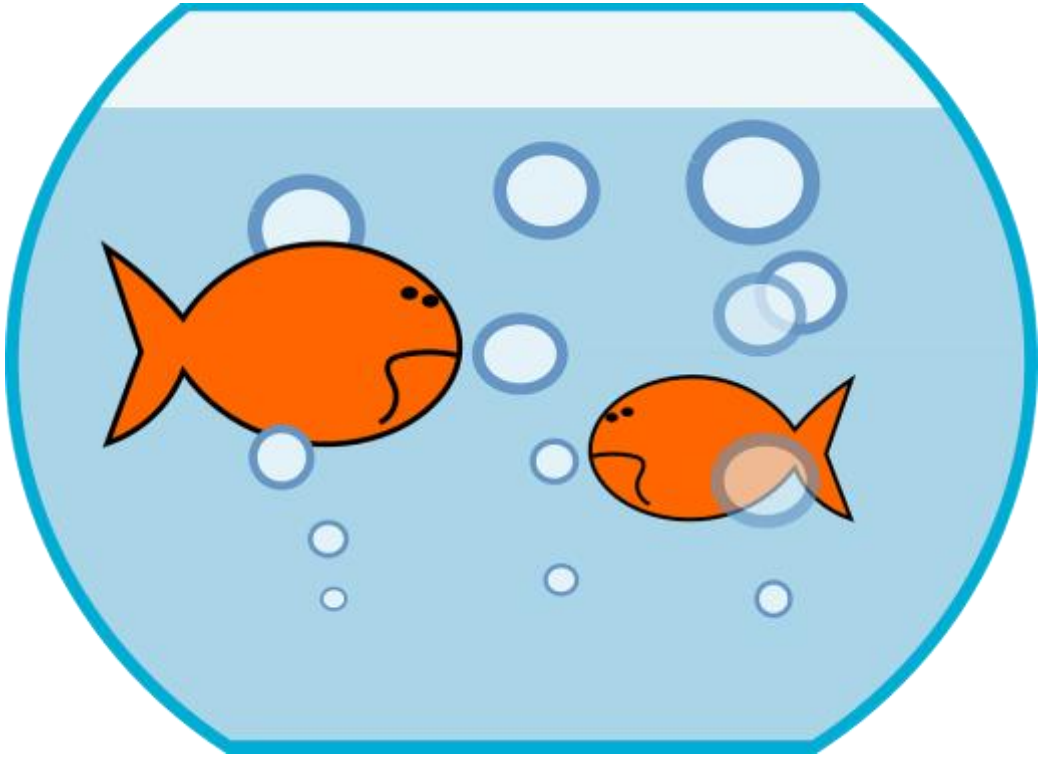
*Dott. R. Grieco*


HAL 9000
PRIVACY

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say"

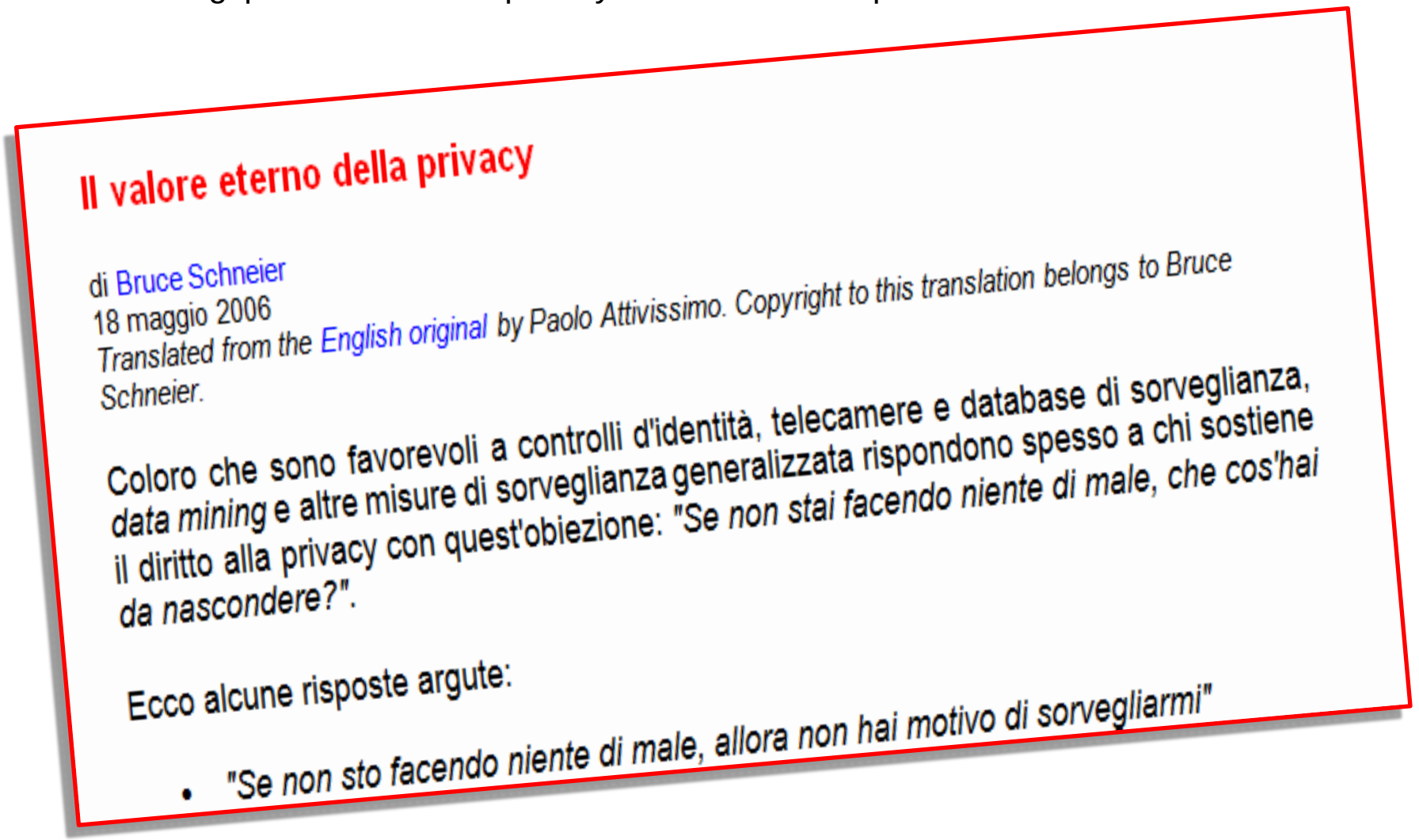
*Edward Snowden*

*"Sostenere che non ti curi della privacy perchè non hai niente da nascondere è come dire che non t'importa della libertà di espressione perchè non hai niente da dire"*



## lettura obbligatoria

attivissimo.blogspot.com/2006/05/privacy-e-intercettazioni-parla.html?m=0



### Il valore eterno della privacy

di Bruce Schneier
18 maggio 2006
*Translated from the English original by Paolo Attivissimo. Copyright to this translation belongs to Bruce Schneier.*

Coloro che sono favorevoli a controlli d'identità, telecamere e database di sorveglianza, *data mining* e altre misure di sorveglianza generalizzata rispondono spesso a chi sostiene il diritto alla privacy con quest'obiezione: "Se *non stai facendo niente di male, che cos'hai da nascondere?*".

Ecco alcune risposte argute:

- "Se *non sto facendo niente di male, allora non hai motivo di sorvegliarmi*"

# PROFILAZIONE

# Com'è facile rubare un'identità Il 99% dà i suoi dati a sconosciuti

**ROMA - Rivelereste nome, cognome, data di nascita, nome dei vostri figli, del vostro cane e quello da nubile di vostra moglie a uno sconosciuto? Se la vostra risposta è no, siete in netta minoranza. Un esperimento condotto a Venezia da un'azienda del ramo della sicurezza online ha scoperto infatti che il 99% delle persone non ha problemi a farlo, a patto di ricevere un giornale in regalo.**

**MA CHE VUOLE?** Sembra chiederselo la signora: la voglia di rispondere è però spesso troppo forte.

L'esperimento era molto semplice. Un gruppo di falsi intervistatori, con il logo di un inesistente tour operator, si avvicinava ai turisti con la scusa di un sondaggio sulle loro preferenze turistiche. Quale "risarcimento" per il tempo sottratto, gli intervistatori offrivano una copia omaggio di un giornale. E con questo stratagemma riuscivano a strappare ai turisti informazioni di ogni tipo. Il 99% di loro, ad esempio, non aveva problemi a fornire il proprio nome. Sull'indirizzo cedeva solo uno su due, mentre quasi l'80% rivelava il cognome da nubile della moglie e oltre l'85% il nome dei figli. Un po' più di riserbo solo per telefono ed e-mail (25%): ma solo per il terrore di essere sommersi di mail-spazzatura. A quasi nessuno (o meglio: solo a uno su 100) è venuto il sospetto che rivelare il proprio nome a uno sconosciuto rappresentasse un problema per la propria sicurezza (o, alla meglio, per i propri soldi). Ed è proprio sull'irresistibile voglia di raccontarsi che fanno leva le trappole dei cyber-pirati, coloro che "rubano l'identità" digitale delle persone attraverso il cosiddetto *phishing* - le mail con falsa intestazione autorevole (ad esempio dalla propria banca) che chiedono informazioni riservate, come la propria password. "Questa indagine dimostra come il fattore umano sia la causa principale del dilagare delle truffe online", ha detto il responsabile della Rsa Security, l'azienda che ha compiuto l'esperimento. Che ha anche specificato come a tutti gli intervistati siano poi stati restituiti i dati, insieme a una mini guida su come evitare di abboccare di nuovo. E chissà se, alla fine, quel giornale gratuito gliel'hanno poi dato. (ANSA)

## Le dieci regole contro i cyber-pirati

1. Non dire a nessuno le tue password. E non annotarle su foglietti alla portata di tutti.
2. Non usare sempre la stessa password. E cambiala ogni 90 giorni.
3. Usa password di almeno 8 caratteri (lettere e numeri).
4. Non usare come password combinazioni di tasti vicini sulla tastiera (es: qwert).
5. Non dare informazioni personali a sconosciuti.
6. Se te ne vengono chieste, chiedi quale uso ne sarà fatto...
7. ...e i recapiti di chi te le chiede (numero di telefono e indirizzo).
8. Chiedi alla banca online se offre strumenti più sicuri di una password.
9. Se acquisti online, verifica che, in basso sullo schermo, compaia un lucchetto.
10. Non dare mai i tuoi dati riservati via mail.

esperimento

## *RAI - Digital world*

iscrizione a finto social con clausola sul primogenito

## LA TOP 50 DEI TRACKER DI DATI

La nostra analisi mette in luce quanti tracker registrano le nostre visite sui 100 principali siti tedeschi (a sinistra). L'elenco qui sotto evidenzia quante pagine un tracker analizza, direttamente o indirettamente (tramite un altro tracker) e non fornisce pertanto le dimensioni esatte di questo circolo

| Posto | Tracker | Pagine tracciate | Azienda di controllo |
|---|---|---|---|
| 1 | googleanalytics.com | 87 | Google |
| 2 | qservz.com | 74 | Quisma |
| 3 | scorecardresearch.com | 73 | TMRG |
| 4 | atdmt.com | 73 | Microsoft |
| 5 | adition.com | 70 | Virtual Minds AG |
| 6 | googleadservices.com | 70 | Google |

## Nel mercato miliardario della pubblicità online, ogni vostro clic viene analizzato. A meno che non vi difendiate

DI CLAUDIO MÜLLER

Un giro di shopping in città può essere snervante: negozi sovraffollati, bambini lamentosi, i pantaloni perfetti disponibili solo nella taglia sbagliata. Tuttavia, gli acquisti "analogici" presentano anche dei vantaggi: infatti non si viene seguiti costantemente da loschi figuri che tengono traccia di ogni nostro passo e di ogni capo di abbigliamento provato. Un'immagine che può apparire spaventosa, ma è proprio questo che succede su internet.

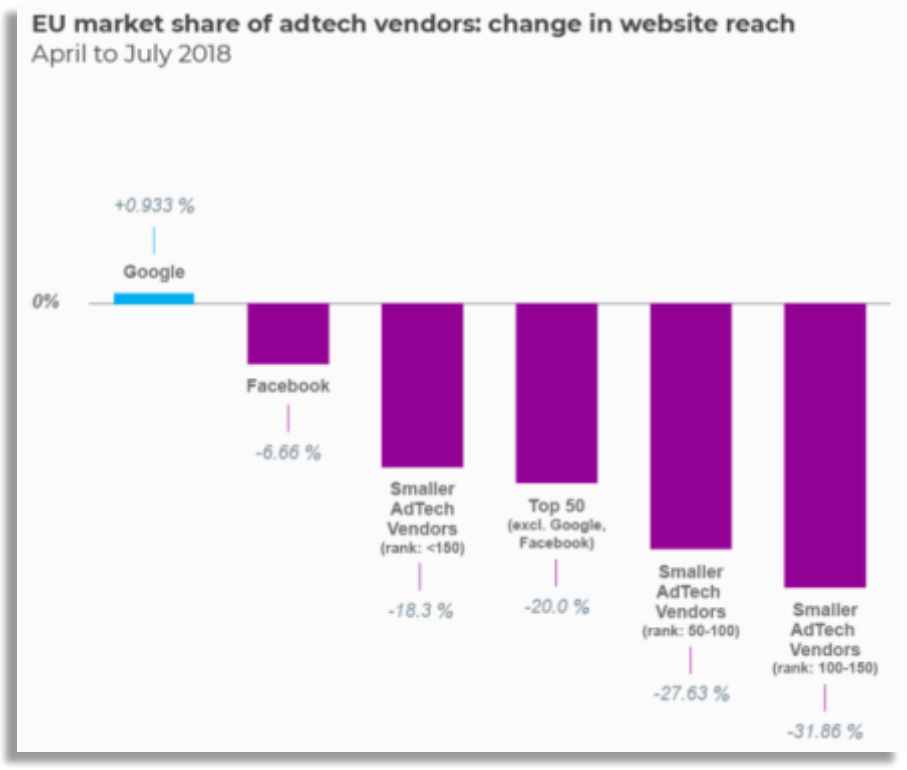
A spiarci sono aziende che inseriscono la pubblicità sui siti e analizzano il comportamento degli utenti, prima su tutti Google. Gli stru-


3 ELEMENTI
3 LIVELLI
OSCILLANTE
GLI ARTICOLI DI QUESTA
VETRINA SI POSSONO
ACQUISTARE CON QUESTI
PREZZI SOLO MOSTRANDO
L'APPLICAZIONE
SCARICATA SUL CELLULARE
3.00
4.80
4.000
9.00
13.00
1.00

# Pubblicità, la GDPR "fa fuori" le piccole aziende e Google vince

I tracker per tracciare l'utente online sono stati ridotti dopo l'entrata in vigore del GDPR. Tutte le aziende (anche Facebook) hanno ridotto il numero di tracker online e la portata dei propri siti. Tranne una: Google.

www.dday.it/redazione/28217/gdpr-ad-tracker-google



# Il profilo dei nostri figli

*Quando cedere alla tentazione di proiettare la propria felicità sugli altri costituisce il primo tassello per la profilazione dei più piccoli.*

www.punto-informatico.it/profilo-nostri-figli/

# Privacy, i prodotti tecnologici da evitare se non vuoi essere "spiato"

*...il portale di Mozilla Foundation chiamato "privacy not included" (la privacy non è inclusa) ...*

www.dday.it/redazione/28677/privacy-dispositivi-dati-smart-speaker-console-tablet

# Usate app di incontri?

Probabilmente il vostro profilo è già stato venduto

www.zeusnews.it/n.php?c=26837

ROMA
QUOTIDIANO D'INFORMAZIONE FONDATO NEL 1862
www.ilroma.net LUNEDÌ 9 GIUGNO 2014 • ANNO CLII N.157 • NUOVA SERIE • € 1,00

Ballottaggi, ecco i sindaci eletti a Nola, Somma Vesuviana, Sant'Anastasia, Marigliano, Pompei e Torre del Greco

**NAPOLI** Una "App" per cellulari con le coordinate satellitari di ogni prostituta

# La mappa delle "lucciole" online con i voti dei clienti

Schianto in moto senza casco, morto 34enne vicino ai Falanga

Registrazione anonima e accesso a migliaia di

POMIGLIANO
Bambino usato come corriere

2018/12/07

## 500 milioni di account rubati a Marriott, Sheraton e altre catene di alberghi

attivissimo.blogspot.com/2018/12/500-milioni-di-account-rubati-marriott.htm

2018/12/07

## Quora, 100 milioni di account violati

attivissimo.blogspot.com/2018/12/quora-100-milioni-di-account-violati.html

# remare contro

## La Five Eyes invoca una backdoor per i dispositivi

*L'alleanza formata da Stati Uniti, Canada, Australia, Regno Unito e Nuova Zelanda chiede alle tech companies l'inclusione di una backdoor nei device.*

www.punto-informatico.it/five-eyes-backdoor-dispositivi/

## In Australia una legge contro la crittografia. Arrivano le backdoor di stato?

*Il governo australiano ha varato una legge che obbliga le aziende a collaborare con la polizia per violare i sistemi o impiantare spyware.*

www.securityinfo.it/2018/12/10/in-australia-una-legge-contro-la-crittografia-arrivano-le-backdoor-di-stato/

# IoT


SAMSUNG
Samsung Smart Washer
Smart Control
Denim
01 H 09 M Left
Est. finish time PM 8:26
Load Sensing
Cancel
Pause

# telecamere

**Telecamere via Internet vulnerabili, alcune mandano da sole i video a qualcun altro**

*www.zeusnews.it/n.php?c=26534*

**Il sito dei guardoni: 73mila telecamere private hackerate**

*www.zeusnews.it/n.php?c=22049*

**Tappate la webcam, lo fanno anche gli esperti**

*www.zeusnews.it/n.php?c=19070*

# Cayla

# Anche le lavatrici oggi sono un obiettivo per i cybercriminali

*Kaspersky: triplicata nel 2018 la crescita dei malware della Internet delle Cose.*

# Are the Police Using Smart-Home IoT Devices to Spy on People?

*IoT devices are surveillance devices, and manufacturers generally use them to collect data on their customers. Surveillance is still the business model of the Internet, and this data is used against the customers' interests: (...)*

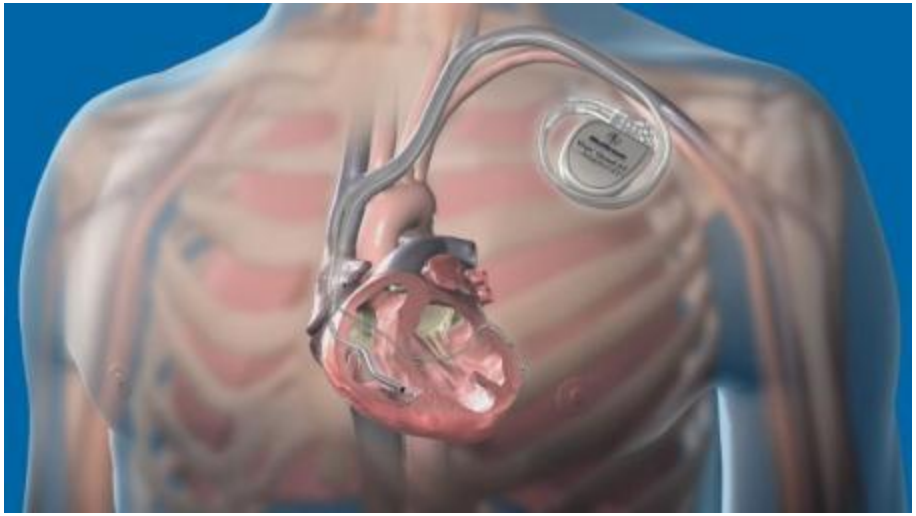
*TechCrunch asked a bunch of companies about this, and basically found that no one is talking.*

www.schneier.com/blog/archives/2018/10/are_the_police_.html

# Falle nei dispositivi medici, così gli hacker possono fermare un pacemaker

*È stato dimostrato alla Black Hat Conference.*

www.zeusnews.it/n.php?c=26604



# Grindr dice ad aziende di terze parti se i suoi utenti sono sieropositivi

***Grindr** ha condiviso informazioni delicate sullo stato di salute dei suoi utenti, in particolare **se avevano l'HIV o meno**, con almeno **due aziende, ovvero Apptimize e Localytics**. È quanto emerge da un'inchiesta di BuzzFeed corroborata dalla ONLUS norvegese SINTEF.*

mobile.hdblog.it/2018/04/03/grindr-hiv-privacy/

# CCleaner, pioggia di critiche per la raccolta dei dati degli utenti

*Il software di Avast è stato paragonato a uno spyware.*

www.zeusnews.it/n.php?c=26587

# Ci sono 9 milioni di telecamere Xiongmai accessibili a chiunque

*Pirati informatici o semplici guardoni possono accedere in un attimo a tutti i dispositivi di sorveglianza del maggior produttore al mondo.*

www.securityinfo.it/2018/10/10/ci-sono-9-milioni-di-telecamere-xiongmai-accessibili-a-chiunque/

# difendere la privacy

step 1: sicurezza informatica

step 2: sensibilizzare gli utilizzatori

step 3: controllare

lettura:
fattore umano

# sicurezza informatica

- sicurezza di rete [>]
- sicurezza delle PdL [>]
- sicurezza delle comunicazioni [>]
- sicurezza dei dati [>]

- risorse umane [>]

# Fra i modi per tutelare la privacy

- un **proxy** per la connessione del client che mascheri il vero IP dell'utente,
- una **rete di anonimato**, come quella offerta dal programma Tor (in cui il proxy è comunque incluso),
- servizi che creano una **Virtual Private Network**,
- **Crittografia, pseudonimizzazione** e offuscamento di protocollo,
- una **block-list** degli indirizzi IP ritenuti malevoli da inserire nel client stesso (qualora esso supporti tale funzionalità),
- caricare **liste** di server da siti che certificano i server e i contenuti.

# This SIM Card Forces all of Your Mobile Data Through Tor

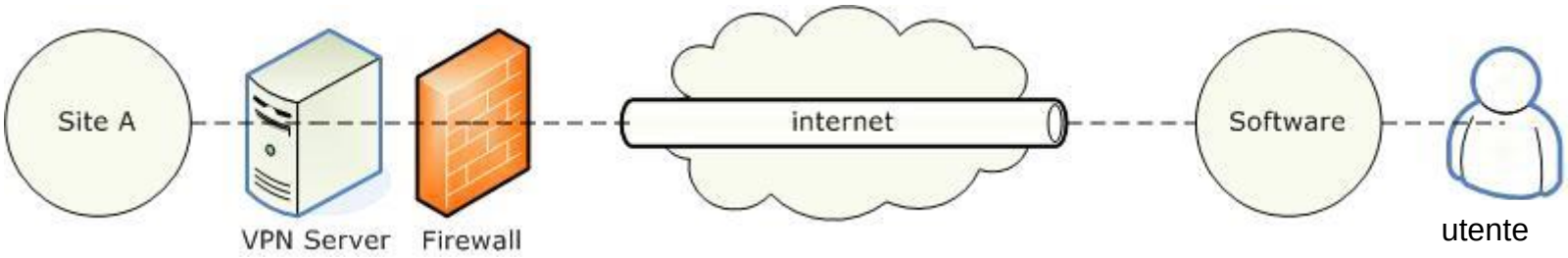
*"This is about sticking a middle finger up to mobile filtering, mass surveillance."*

motherboard.vice.com/en_us/article/d3qqj7/sim-card-forces-data-through-tor-brass-horn-communications

# usare una VPN per connettersi

difficoltà: 6 > 3

VPN - Virtual Private Network; connessione criptata fra 2 punti (noi e la controparte)



19 ottobre, 2018

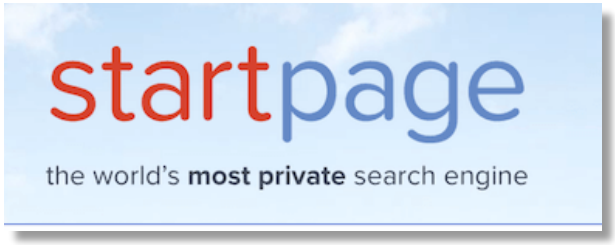
# Data privacy: i tuoi dati al sicuro anche in viaggio

vocearancio.ing.it/va-data-privacy-dati-al-sicuro-in-viaggio/?tc=email-VA-lavoro-va-data-privacy-dati-al-sicuro-in-viaggio-241018

- Attenti alle promesse del Wi-Fi libero
- Gli argini contro le invasioni (HTTPS, VPN, 2-factor)
- Preparatevi al confine.
- Dispositivi puliti e cloud protetti.

# Raccomandazioni per gli utenti

usare motori di ricerca non *ficcanaso*:



difficoltà: 1 > 9

# spioni

*The standard search engines (Google, Bing, Yahoo, etc.) track and record everything you search for. Your typical search engine records the following information any time you use it:*

- Your IP address
- User agent
- Unique identifier (stored in browser cookies)
- Search terms

# libri

*Una nota che riguarda la navigazione WWW: se privacy e anonimato sono le vostre priorità dimenticatevi per sempre di Google e affini e puntate su motori di ricerca che non vi monitorano come* ***DuckDuckGo*** *oppure* ***StartPage****.*

*Perché? Prendiamo per esempio Youtube.* Youtube *è un servizio acquistato e gestito da Google e Google, lo sappiamo, traccia qualunque cosa. Youtube prende nota di qual è il tuo IP e quale video stai vedendo, quindi butta giù un profilo utente chiamato* fingerprint *e sa già cosa ti piacerebbe vedere dopo o magari acquistare mentre visiti siti web con Google Adwords. Un circolo vizioso.*

Hacklog - manuale sulla sicurezza informatica e Hacking etico

# spioni

- browserleaks.com/
- gizmodo.com/heres-all-the-data-collected-from-you-as-you-browse-the-1820779304
- **http://webkay.robinlinus.com/**
- www.techlicious.com/tip/how-browsers-leak-personal-information/

# utenti (~)

usare con discernimento Google e i suoi servizi:

- Gmail
- Maps
- StreetView
- Google Earth
- google drive
- ...

difficoltà: 0 / 9

(ma anche gli altri)

# utenti (~)

- respingere i cookies ovunque possibile e comunque cancellarli il più spesso possibile; certamente alla chiusura del browser
- idem per la cronologia
- bloccare gli script
- usare account anonimi ***consapevolmente***
- ...

# CONSIGLI
## contro la raccolta di dati

Con pochi clic potete limitare il tracciamento sul web, cancellare i supercookie e mettere al sicuro il vostro cellulare

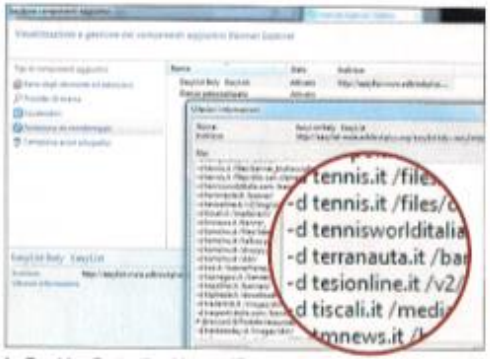
Sfuggire completamente al tracciamento dei dati è impossibile. Con i nostri consigli potete però limitare questa raccolta di informazioni in maniera da impedire la creazione di profili utente su di voi che siano di una qualche utilità. Al tempo stesso potete sfruttare la Rete senza dover fare delle rinunce in termini di comfort. Se volete informarvi ancora prima di visitare una pagina, potete sfruttare il motore di ricerca cookie **b-versio.verbraucher-sicher-online.de/jcookie/index.jsp**. Questo progetto dell'Università di Berlino mostra tutti i cookie di una pagina e altre informazioni sui servizi di tracciamento.

**Cancellare i cookie (IE, Firefox, Chrome)** I cookie Http possono essere cancellati direttamente tramite il browser. In Internet Explorer andate in Strumenti/Sicurezza/Elimina cronologia esplorazioni e mettete un segno di spunta su Cookie e dati siti Web. Firefox offre questa opzione in Opzioni/Privacy/Rimuovere singoli cookie/Rimuovi tutti i cookie. In Chrome andate in Impostazioni/Mostra impostazioni avanzate/Privacy/Cancella dati di navigazione. In Privacy/Impostazioni contenuti/Cookie potete anche far sì che i cookie vengano automaticamente cancellati quando chiudete il browser. In questo modo però non vi liberate dei cookie Flash: per questi serve un componente aggiuntivo come BetterPrivacy (Firefox) o Click&Clean (Chrome). Questi tool trovano e cancellano anche i supercookie ogni volta che chiudete il browser. BetterPrivacy non richiede alcuna impostazione mentre in Click&Clean dovete rimuovere il segno di spunta su Disattiva in Cancella dati privati.

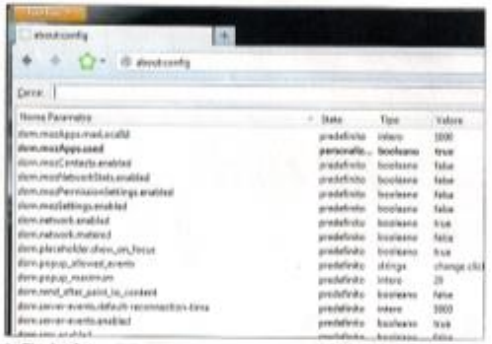
**Disattivare il Dom storage (Firefox)** Soltanto Firefox vi consente di disattivare la memorizzazione di dati delle applicazioni web nel browser (Dom storage). Digitate *about:config* nella riga dell'indirizzo, cercate il parametro dom.storage.enabled e cliccateci sopra due volte. In questo modo la voce viene impostata su False e i siti web non possono più salvare i dati.

**Attivare gli elenchi di tracker (Internet Explorer)** In Internet Explorer, la migliore protezione contro i tracker dei dati è la Tracking Protection List. Varie liste sono disponibili all'indirizzo **www.iegallery.com/it-it/trackingprotectionlists**. L'elenco può essere installato in IE (versione 9 o superiore) come plug-in. In questo modo tutti i tracker elencati vengono bloccati non appena si attivano su un sito web. Le liste vengono generalmente aggiornate periodicamente così da essere sempre all'avanguardia.

**Configurare i dispositivi mobili (Android, iOs)** Dalla fine di novembre è disponibile per gli smartphone Android l'app Adblock Plus contro la pubblicità, che blocca gli annunci sui siti mobile ma anche i banner nelle apps. Inoltre, dovreste disattivare la funzione di localizzazione Gps del vostro apparecchio se non vi serve assolutamente. In iOS, dalla versione 6 potete pur sempre limitare il tracciamento a fini pubblicitari. Andate in Impostazioni/Generali/Info/Promozione/Limita AD Tracking.




**La Tracking Protection List per IE trova e blocca i tracker sui siti web sulla base di dati aggiornati regolarmente**



**In Firefox è possibile disabilitare con un doppio clic la memorizzazione dei dati (Dom storage) tramite le impostazioni di about:config**


**In Android bisognerebbe disattivare la localizzazione Gps poiché i servizi di tracciamento spesso e volentieri collegano questi dati ai profili degli utenti**

# hardware vario

Scopri se la tua stampante ti spia

www.zeusnews.it/n.php?c=8536

Quando la stampante fa la spia, l'UE si sveglia

Stampanti spione: l'Unione Europea si muove un pochino.

www.zeusnews.it/n.php?c=6942

Se la tua fotocopiatrice ti manda una mail, non aprirla con un vecchio Word

www.zeusnews.it/n.php?c=25193

# *M4.1* – Sicurezza del trattamento dati

## *Le finalità dell'IT Security*

# IT SECURITY

insieme di tecniche, politiche e norme mirate a proteggere i Sistemi informatici

ma soprattutto i **dati** in essi contenuti

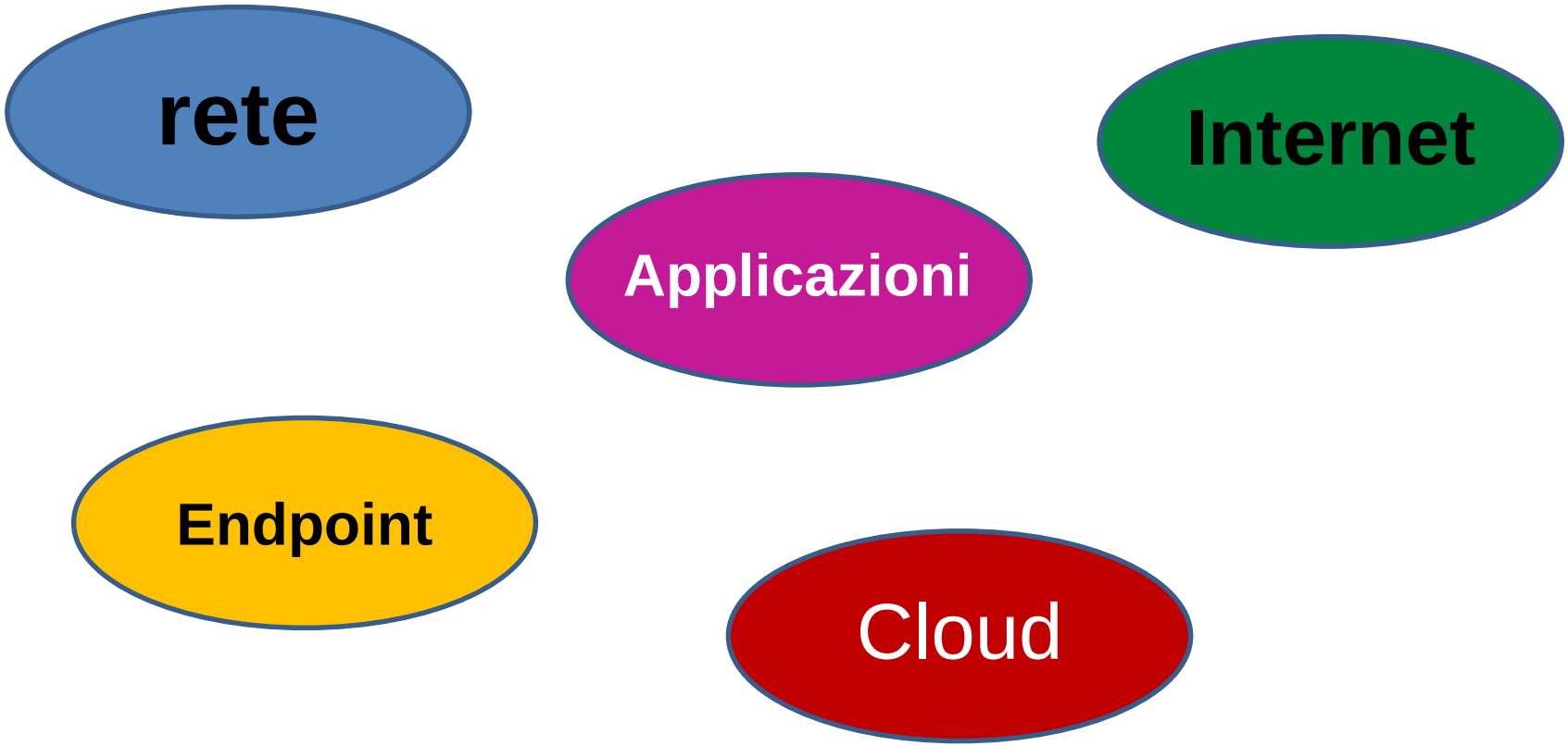
# Perchè si attacca un sistema informatico?

- apportare danni
- rubare dati o denaro
- alterare dati
- bloccare un servizio
- accedere a risorse riservate
- lanciare un attacco a terzi (DDoS)

# Tecniche di attacco

- Hacking (...)
- Buffer overflow
- DoS e DDoS
- **Ingegneria sociale**
- Keylogging
- Backdoor
- Spoofing
- Social Network Poisoning
- **Spyware e malware**

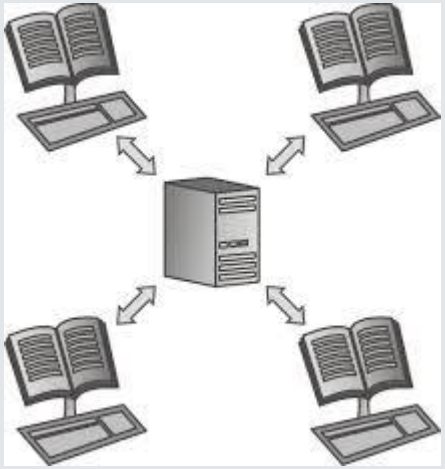
# ambiti di sicurezza



# *M4.1* – Sicurezza del trattamento dati

## *La tecnologia Peer to Peer*

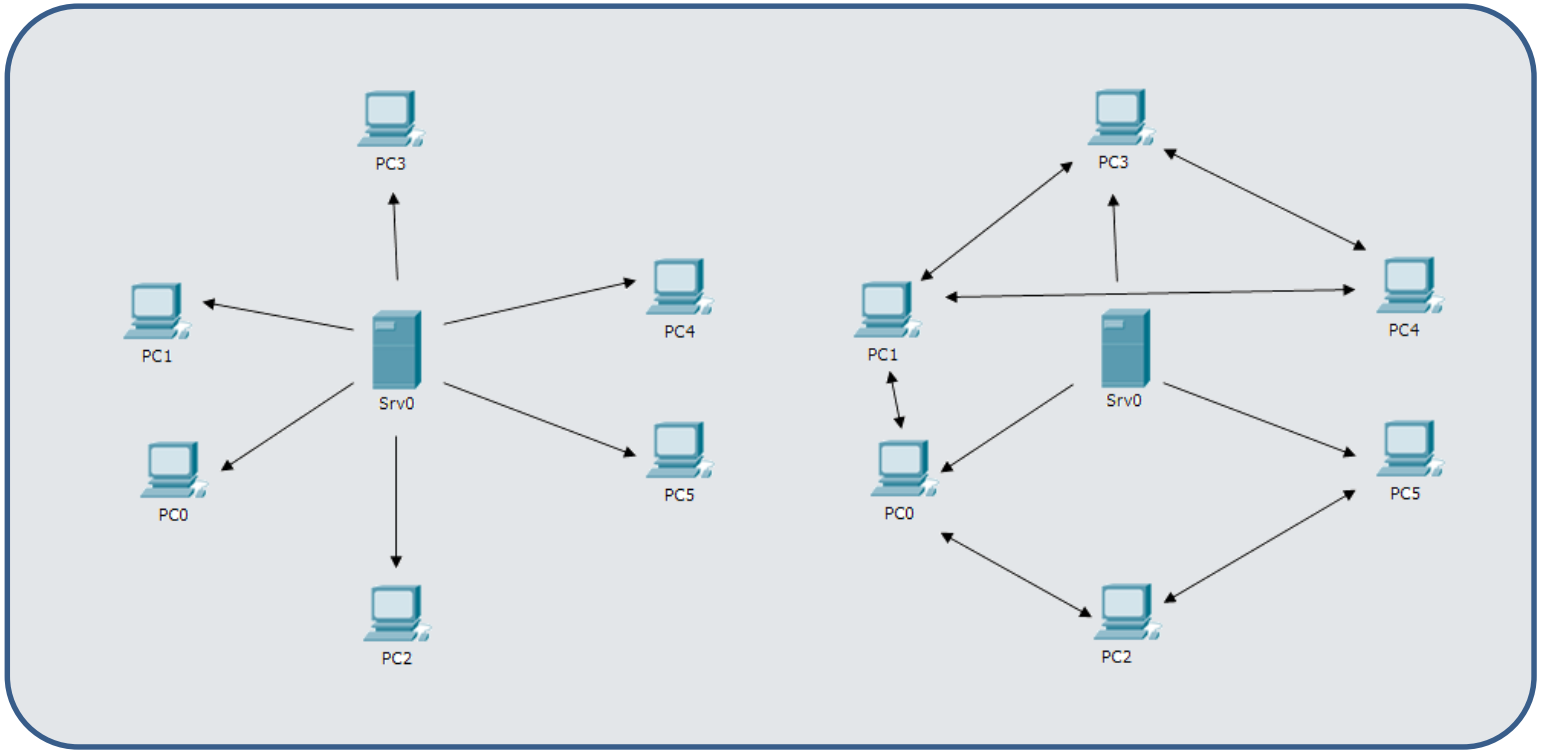
# Che cos'è il Peer-to-Peer (P2P)?



Server

client

# Che cos'è il Peer-to-Peer (P2P)?




Un nodo P2P può fungere da server e client allo stesso tempo

# Storia

Primi scambi con reti come **Fidonet**;

Il primo P2P in senso stretto fu **NAPSTER**; creato nel giugno 1999 e fieramente osteggiato dall'industria dell'intrattenimento (dicembre), si è fermato nel 2001.

2000 - Gnutella, eDonkey, Freenet

2001 - Kazaa, Morpeus, BitTorrent

…

# Situazione attuale

oggi esistono molti protocolli per lo scambio P2P e i relativi programmi:

- Acquisition
- Aimster
- Ares
- Ares Lite
- BitTorrent
- Blubster
- Direct Connect
- eDonkey 2000 e Overnet
- FreeWire
- Gnucleus
- Grokster
- GTK-Gnutella
- iMesh
- Kazaa Lite, Kazaa Lite K++
- Kazaa Media Desktop
- LimeWire
- Mactella
- mIRC
- Morpheus
- NeoNapster
- OneMX
- Phex
- Piolet
- Qtella
- Shareaza
- SoulSeek
- TrustyFiles
- WarezP2P
- WinMX
- XoLoX

# Rischi del peer-to-peer

Un programma P2P rappresenta un rischio per vari aspetti:

- utilizza porte lasciate aperte
- mette in contatto con computer non controllati
- riceve file potenzialmente dannosi
- occupa la banda dell'organizzazione
- ...

# Rischi del peer-to-peer

Porte usate

kazaa - fasttrack: TCP/UDP 1214;

edonkey: TCP/UDP 4661-4672;

winmx e napster: TCP/UDP 6257 e 6699;

bittorrent: TCP/UDP 6881-6889;

gnutella: TCP/UDP 6346

# Rischi del peer-to-peer

Nei circuiti P2P è diffusa l'usanza di alterare i file, soprattutto i video (film, serie, documentari, cartoni)

anche se lo si usa per ottenere materiale legittimo (?), c'è il pericolo di dare p.e. ai bambini del materiale non adatto

# Rischi del peer-to-peer

Per massimizzare il traffico e sincronizzarsi con orari di Paesi lontani si tende a lasciare il PC che fa P2P sempre acceso,

sempre connesso,

sempre con porte aperte e in contatto con potenziali minacce

NB - ragioni di sicurezza *possono* far lasciare il PC acceso, ma senza programmi pericolosi...

# Copyright

Copiare o trasferire contenuti coperti da diritto d'autore senza l'esplicito consenso del titolare dei diritti è illegale

Ma non è il mezzo che è illegale *per se*

# usi leciti

LibreOffice distribuisce il suo software anche tramite i canali peer-to-peer

Distribuzione di materiale lecito/legale ma dal punto di vista sociale o culturale deplorevole, imbarazzante, o contro la morale

paura di essere censurati nel proprio paese

riservare la propria privacy (blog)

"inutile criminalizzare sistemi di file-sharing, nati proprio come strumento collaborativo, laddove è assente una politica aziendale improntata alla sicurezza e alla conoscenza"

*(Punto Informatico - 29 ottobre 2004).*

# DIFESE

- Alcuni protocolli sono cifrati
- Alcuni sono centralizzati, altri completamente distribuiti

# DIFESE

- Chiudere le porte (firewall)
- Bloccare i protocolli
- Monitorare il traffico
- Impedire installazioni a livello dei client
- Utilizzare un tool apposito

www.punto-informatico.it/arrivano-i-tool-castiga-p2p

# *M4.2* – Sistemi informatici integrati e misure di sicurezza

## *Attacchi di Malware*

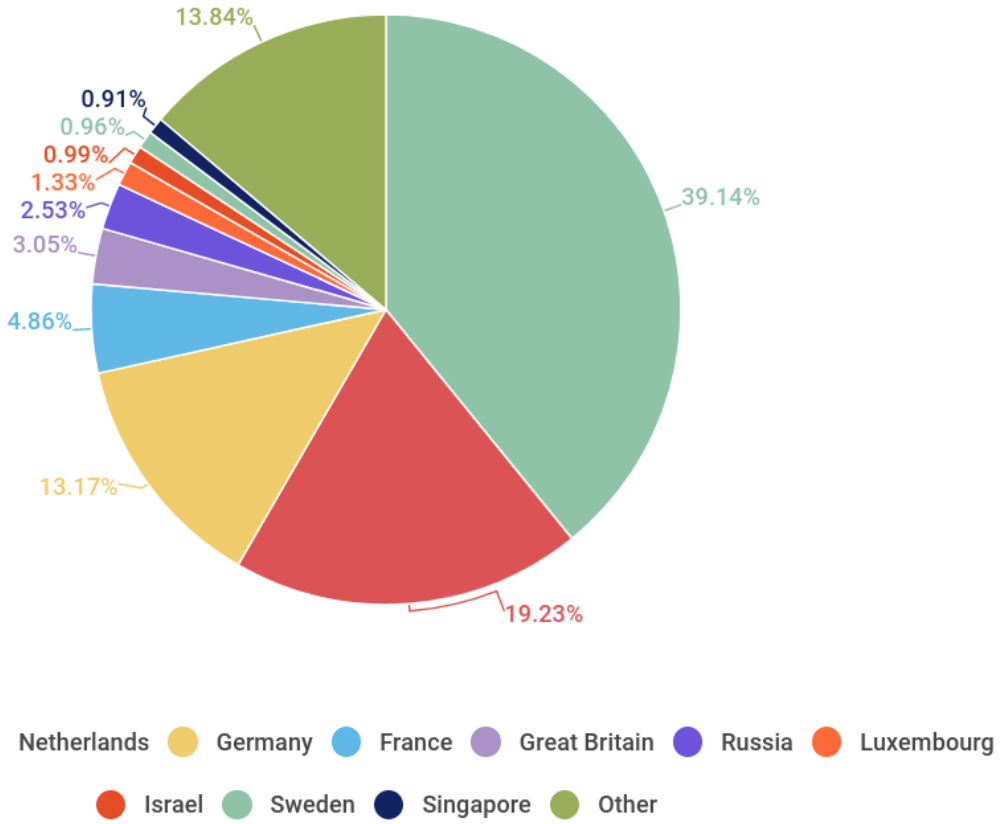
*Dott. R. Grieco*

# MALWARE

software progettato **intenzionalmente** per apportare danni di varia natura a un computer o altre apparecchiature informatiche

- **Virus** (boot virus, MBR, residenti, polimorfici, network, encrypted, spacefiller, macro, web scripts, armored...)
- cavalli di Troia
- ransomware
- Adware
- worms
- spyware
- scareware
- rootkit

eccetera


13.84%
0.91%
0.96%
0.99%
1.33%
2.53%
3.05%
4.86%
39.14%
13.17%
19.23%
United States
Netherlands
Germany
France
Great Britain
Russia
Luxembourg
Israel
Sweden
Singapore
Other

# Perché?

- esperimenti (il *Morris worm*, primo worm diffuso su internet, 1988)
- proteggere diritti (?) (rootkit Sony, 2005)
- causare danni al nemico (Stuxnet, 2007)
- ottenere denaro (CryptoLocker, click fraud, scareware)
- carpire informazioni
- creare una rete per attacchi (DOS, DDOS...)
- ...

# come si diffonde

- insieme a un altro programma (ritenuto innocuo)
- direttamente (da email, siti web, social...)
- macro in documenti di Office Automation

frequente scambiandosi copie abusive

Sono anche arrivati da supporti ufficiali provenienti direttamente dal produttore (rootkit Sony, virus su floppy originali)

# Attacco letale a base di chiavetta USB

L'ingegneria sociale progredisce, facendo leva sulla morbosa curiosità del genere umano. Si aprono altre voragini di sicurezza.

www.zeusnews.it/n.php?c=4881

(...) hanno raccolto una ventina di chiavette USB e vi hanno installato un software-spia per raccogliere login name, password, identificazioni hardware e spedirle via mail a un indirizzo predeterminato.

L'ostacolo maggiore era far finire queste chiavette nelle mani degli operatori della banca. Sono state **seminate nei luoghi più frequentati**, tipo accanto alla macchina del caffè o alla fotocopiatrice. (...)

# esempi celebri

- Petya
- NoPetya
- WannaCry
- Cryptolocker
- ILOVEYOU
- MyDoom
- Stuxnet
- Code Red
- Melissa
- Conficker

**Il malware che cancella gli hard disk ricomincia a far vittime in Italia**

Shamoon è tornato e ha attaccato la Saipem.

www.zeusnews.it/n.php?c=26927

# debolezze

- politica di aggiornamenti inadeguata
- uso incauto di supporti removibili
- uso *allegro* di email e in genere di internet
- lavorare con account administrator
- usare lo stesso S.O. su tutte le macchine
- ...

# difese

- disabilitare avvio da supporti esterni (v.)
- tenere aggiornati antivirus & antimalware
- imporre regole per l'uso di email e internet
- firewall
- filtri web
- proteggere le risorse hardware
  (PC, server, sala server)

# software di protezione

- antivirus
- antyspyware
- antimalware
- firewall
- anti-rootkit
- USB guard
- *[protezione del browser]*
- virtualizzazione

# smartphone

# Migliaia di siti mobile accedono ai sensori dello smartphone senza informare l'utente

www.zeusnews.it/n.php?c=26727

*(...) ben nove browser - Chrome, Edge, Safari, Firefox, Brave, Focus, Dolphin, Opera Mini e UC Browser - consentono ai siti di accedere ai dati dei sensori, senza che l'utente ne sia informato.*

*Per lo meno Mozilla, non appena la notizia s'è risaputa, è intervenuta revocando i relativi permessi a Firefox.*

# Le app ti tracciano anche dopo che le hai disinstallate

*Disinstallare un'applicazione non basta a levarsela di torno. Ci sono servizi, infatti, che continuano il tracciamento di un utente dopo la rimozione dell'app, proponendo pubblicità specificamente create per chi ha disinstallato una certa app.*

www.tomshw.it/smartphone/le-app-ti-tracciano-anche-dopo-che-le-hai-disinstallate/


# Il bug di iOS che permette di sbirciare le foto anche a iPhone bloccato

*Come mostra il sito che riportiamo più sotto, usando i comandi vocali di Siri è possibile accedere alle foto e spedirle via iMessage a un altro dispositivo. Per quanto riguarda i documenti, un procedimento analogo si può usare sfruttando un bug nella funzionalità Quick Look.*

www.zeusnews.it//n.php?c=26773


www.tomshw.it/google-sa-sempre-dove-siamo-anche-quando-non-vogliamo-96692

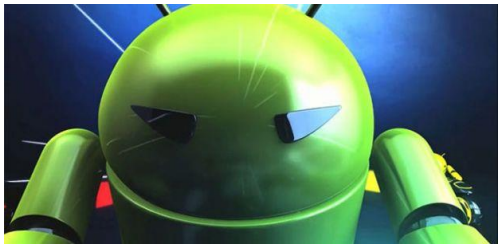
www.wired.it/internet/web/2018/08/13/google-tracciamento-senza-consenso/

Google Tracks its Users Even if They Opt-Out of Tracking
www.schneier.com/blog/archives/2018/08/google_tracks_i.html

## Google ammette: possono cambiare le impostazioni degli smartphone da remoto

E la privacy degli utenti?

www.zeusnews.it/n.php?c=26697



## WhatsApp conferma: i messaggi conservati su Google Drive non sono crittografati

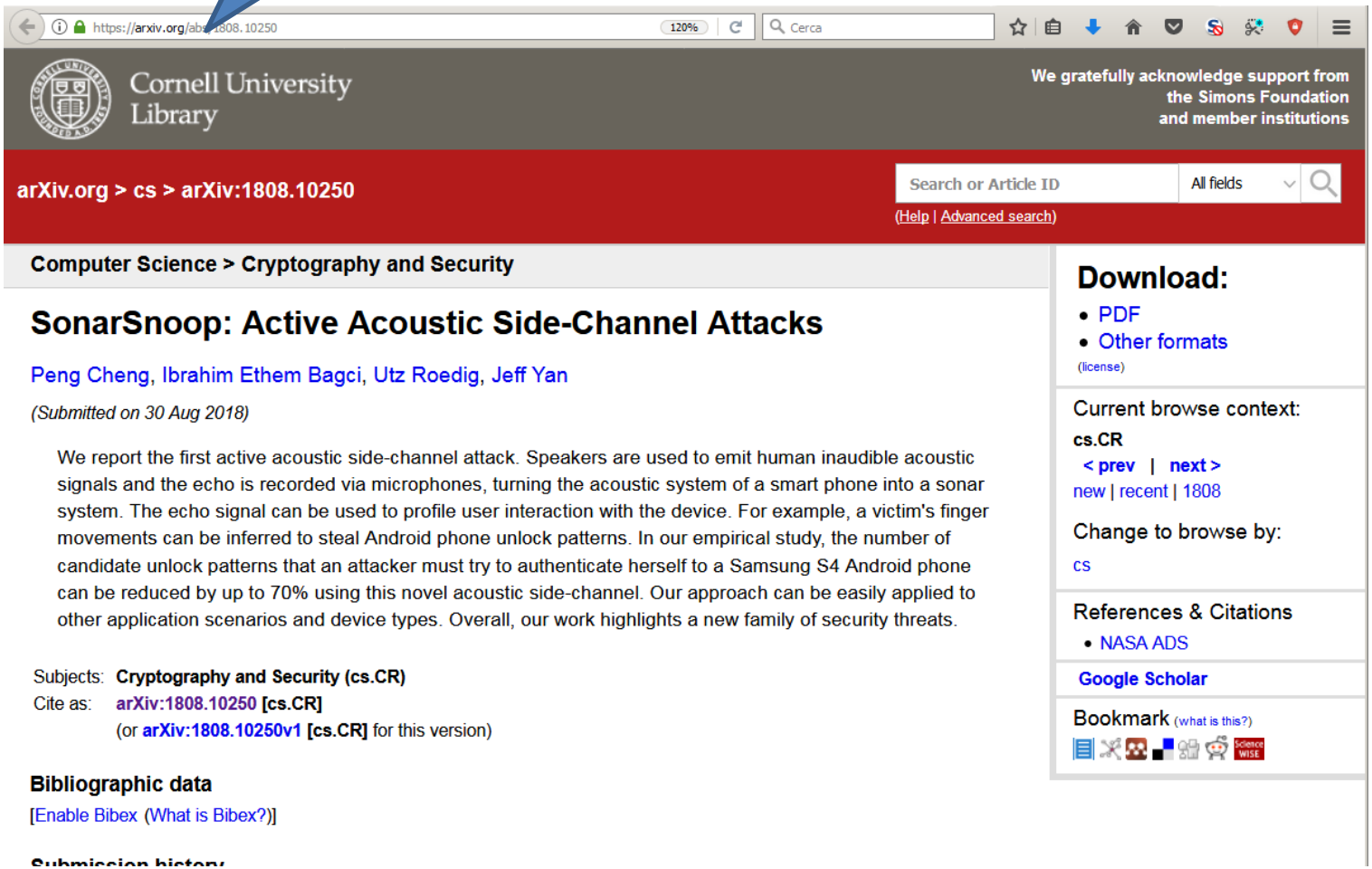
www.zeusnews.it/n.php?c=26658

# Centinaia di giochi per smartphone usano il microfono per spiare gli utenti

*E vendere i dati raccolti ai pubblicitari.*

www.zeusnews.it/n.php?c=26024

arxiv.org/abs/1808.10250



# *M4.2* – Sistemi informatici integrati e misure di sicurezza

## *Minacce Malware*

# hardware

**L'attacco alla Internet delle Cose che può mettere fuori uso la rete elettrica**

*Che succederebbe se degli hacker accendessero da remoto tutti i forni e i boiler della Internet of Things?*

www.zeusnews.it/n.php?c=26625

# Difetti delle CPU

www.tomshw.it/hardware/bug-dei-microprocessori-tutto-su-meltdown-e-spectre/


# Malicious Component Found on Server Motherboards Supplied to Numerous Companies

hackaday.com/2018/10/04/malicious-component-found-on-server-motherboards-supplied-to-numerous-companies/

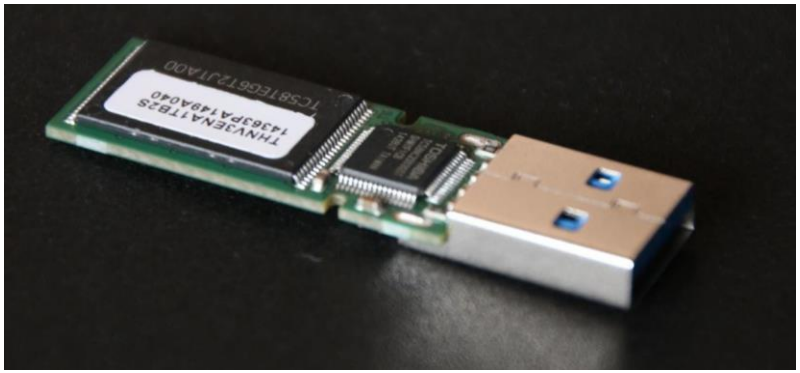
# The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

*The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.*

www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

# BadUSB

attacco a metà tra hardware e software; modifica il firmware di un dispositivo USB per propagare un malware



# BadUSB, nuovo malware invisibile: infetta qualsiasi computer e periferica USB

BadUSB è un nuovo potente malware che infetta computer, mouse, chiavette di memoria e qualsiasi dispositivo dotato di USB. Basta un solo contatto e non è rilevabile.

www.macitynet.it/creato-badusb-pericolosissimo-malware-si-lega-firmware-qualsiasi-dispositivo-usb/

# Dispositivi USB, un disastro per la sicurezza

*Da Israele arriva la "mega-lista" degli attacchi a base di USB, una tecnologia di connessione universale e universalmente usata anche dai cyber-criminali per compiere ogni genere di azione malevola*

www.punto-informatico.it/dispositivi-usb-un-disastro-per-la-sicurezza-2/

# La falla che trasforma i cavi USB per la ricarica in veicoli per il malware

*Con USBHarpoon l'utente non si accorge di niente.*

www.zeusnews.it/n.php?c=26627

Il cavo modificato, all'apparenza, è un normale cavo per la ricarica ma contiene i componenti necessari per portare l'attacco.

# DarkVishnya: attacchi alle banche come nei film di Hollywood

...i pirati hanno usato piccoli computer **Raspberry Pi**, che possono essere nascosti facilmente, e i cosiddetti **Bush Bunny**, dispositivi USB che consentono di ottenere l'accesso al computer a cui vengono collegati e integrano un modem GPRS/3G/LTE.

**In altri casi, addirittura, hanno utilizzato dei computer portatili che hanno collegato alla rete locale e all'alimentazione, abbandonandoli in un angolo di qualche ufficio**.

www.schneier.com/blog/archives/2018/12/banks_attacked_.html

www.securityinfo.it/2018/12/08/darkvishnya-attacchi-alle-banche-come-nei-film-di-hollywood/

securelist.com/darkvishnya/89169/

# WiFi

deve essere ritenuta una connessione a rischio, come pure tutti i dispositivi wireless (tastiera e mouse in primis)

**WPA2 password crack: attacco al WiFi**

*Sfruttare una vulnerabilità del protocollo WPA2 per ottenere in chiaro le informazioni trasferite tramite WiFi: ecco come attuare l'attacco KRACK.*

www.html.it/articoli/wpa2-password-crack-attacco-al-wifi/

**Guida rapida al crack delle reti wireless**

www.megalab.it/4135/guida-rapida-al-crack-delle-reti-wireless-wep-wpa-wpa2

WEP (1999), WPA (2003), WPA2 (2004)...


FREE WI-FI
Pw: 58664452

# vulnerabilità software

- del Sistema Operativo
- degli applicativi
- degli apparati (firmware)
- degli utenti

# Cortana consente agli hacker l'accesso al Pc, anche a sistema bloccato

www.zeusnews.it//n.php?c=26216

www.webnews.it/2018/06/13/cortana-falla-windows-10

www.windowscentral.com/microsoft-patches-major-cortana-lock-screen-bypass-bug-windows-10

www.fastweb.it/web-e-digital/un-bug-di-cortana-rende-inutile-la-password-del-vostro-pc

# HARDENING

*operazioni specifiche di configurazione di un sistema informatico (e dei suoi relativi componenti) che mirano a minimizzare l'impatto di possibili attacchi informatici che sfruttano vulnerabilità dello stesso, migliorandone pertanto la sicurezza complessiva*

wikipedia

# Hardening

In Italia rientra nelle pratiche tecniche introdotte dal *documento programmatico sulla sicurezza 196/03* sulla sicurezza dei dati ed in generale enuncia i criteri da adottare per garantire l'adozione delle misure minime di sicurezza sui sistemi e sulle infrastrutture tecnologiche.

Dal 25 Maggio 2018 ha efficacia il **GDPR**

1) *One Time Hardening:* viene effettuato solo una volta dopo la prima implementazione del sistema

2) *Multiple Time hardening: v*iene effettuato più volte durante la vita del sistema, e la sua ripetizione nel tempo dipende da due fattori fondamentali che sono il rilascio di patch di aggiornamento (patch management) per far fronte alle zero day vulnerability e l'aggiunta di moduli complementari a quello installato di base.

# HARDENING

- chiusura delle porte non indispensabili
- apparecchiature dedicate (firewall)

- arresto di servizi
- disabilitazione di privilegi
- eliminazione di account poco o nulla usati
- disinstallazione di programmi o parti del sistema operativo *(debloating)*

# HARDENING

- limitazione connessioni
- limitazioni di accessi o diritti

- controllo della navigazione (web filtering)
- autenticazione utente con token

# HARDENING

misure a latere

- uso accorto del backup
- cifratura
- sorveglianza

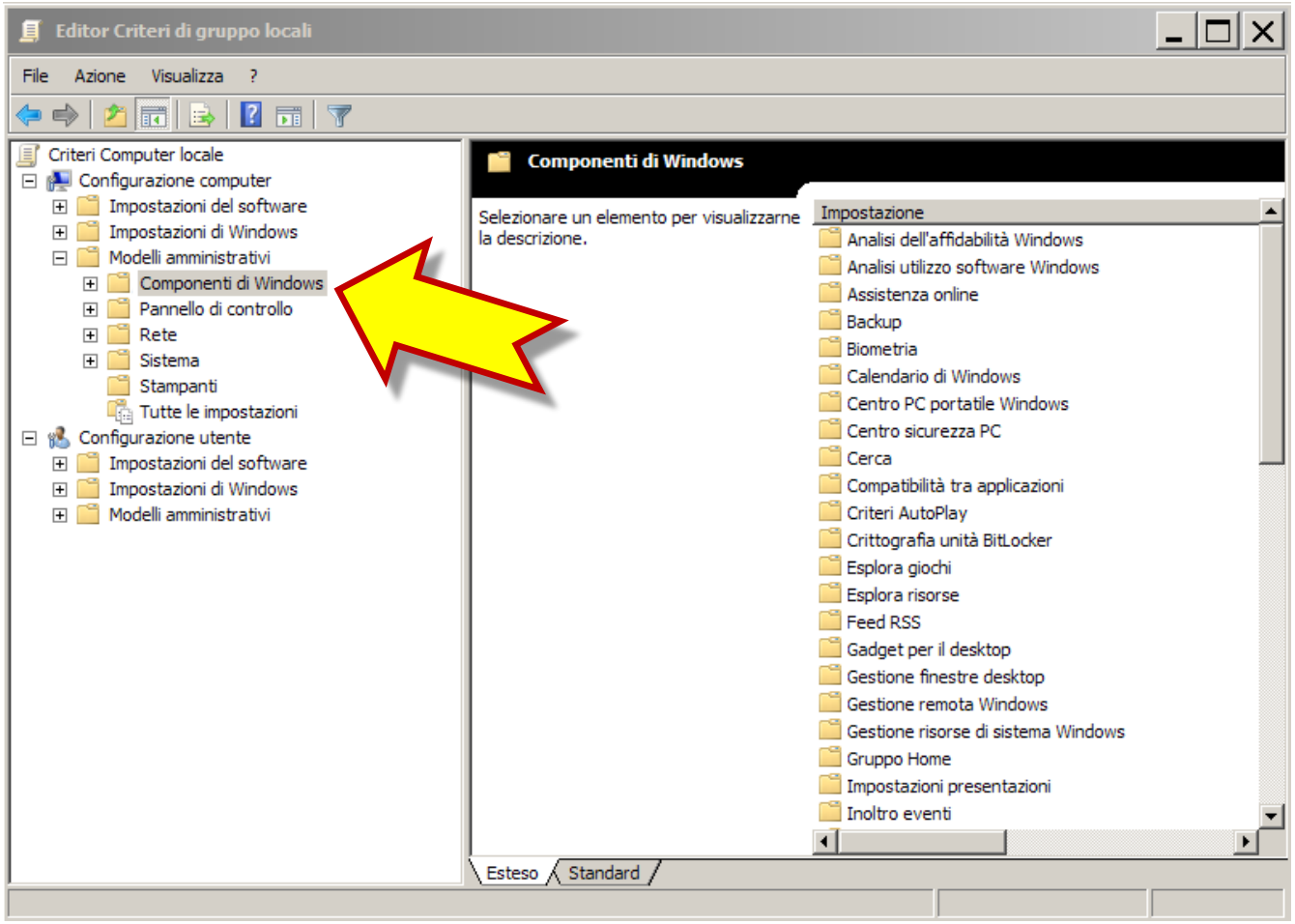
# esempio domestico

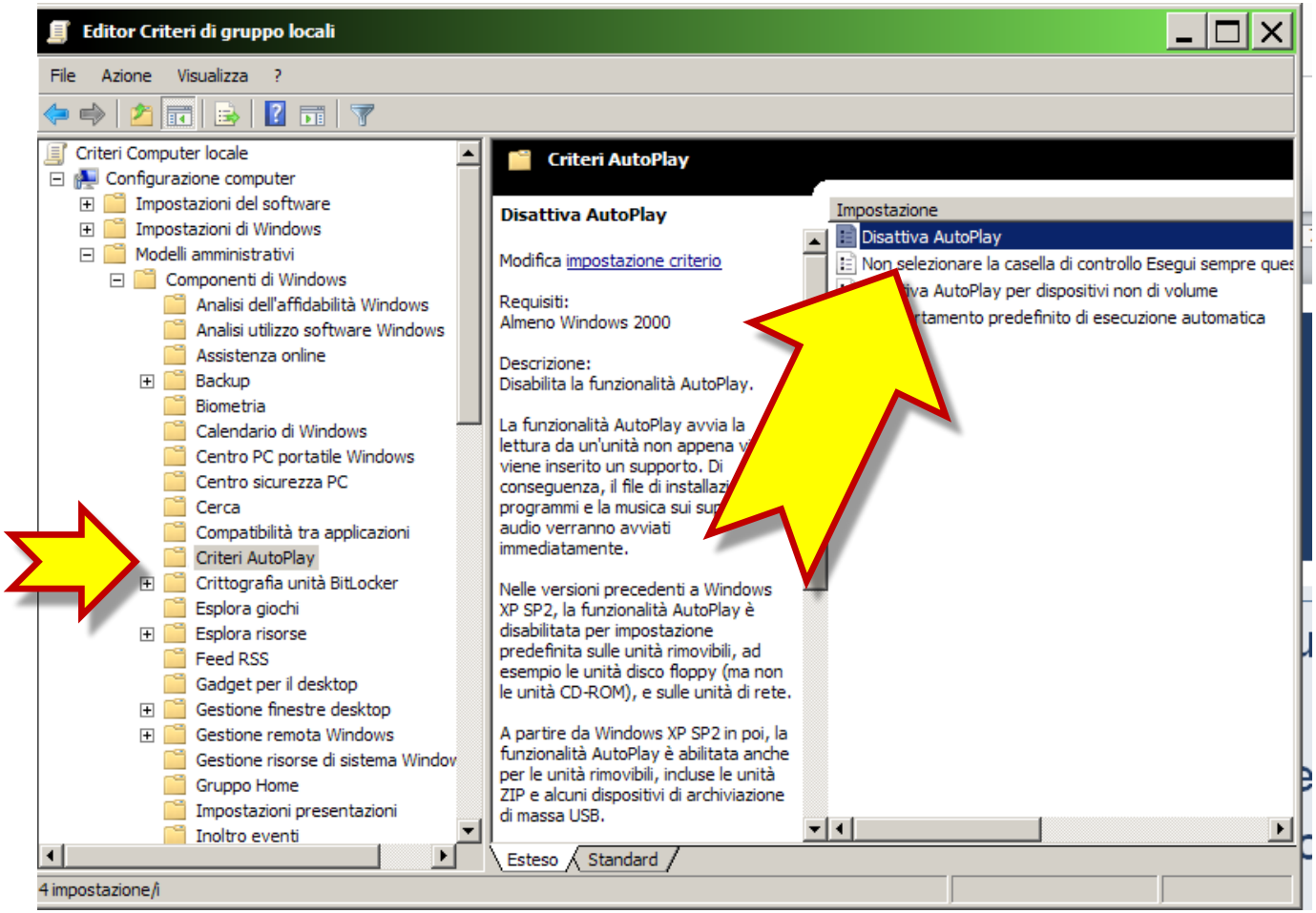
per disabilitare l'autorun (esecuzione automatica):

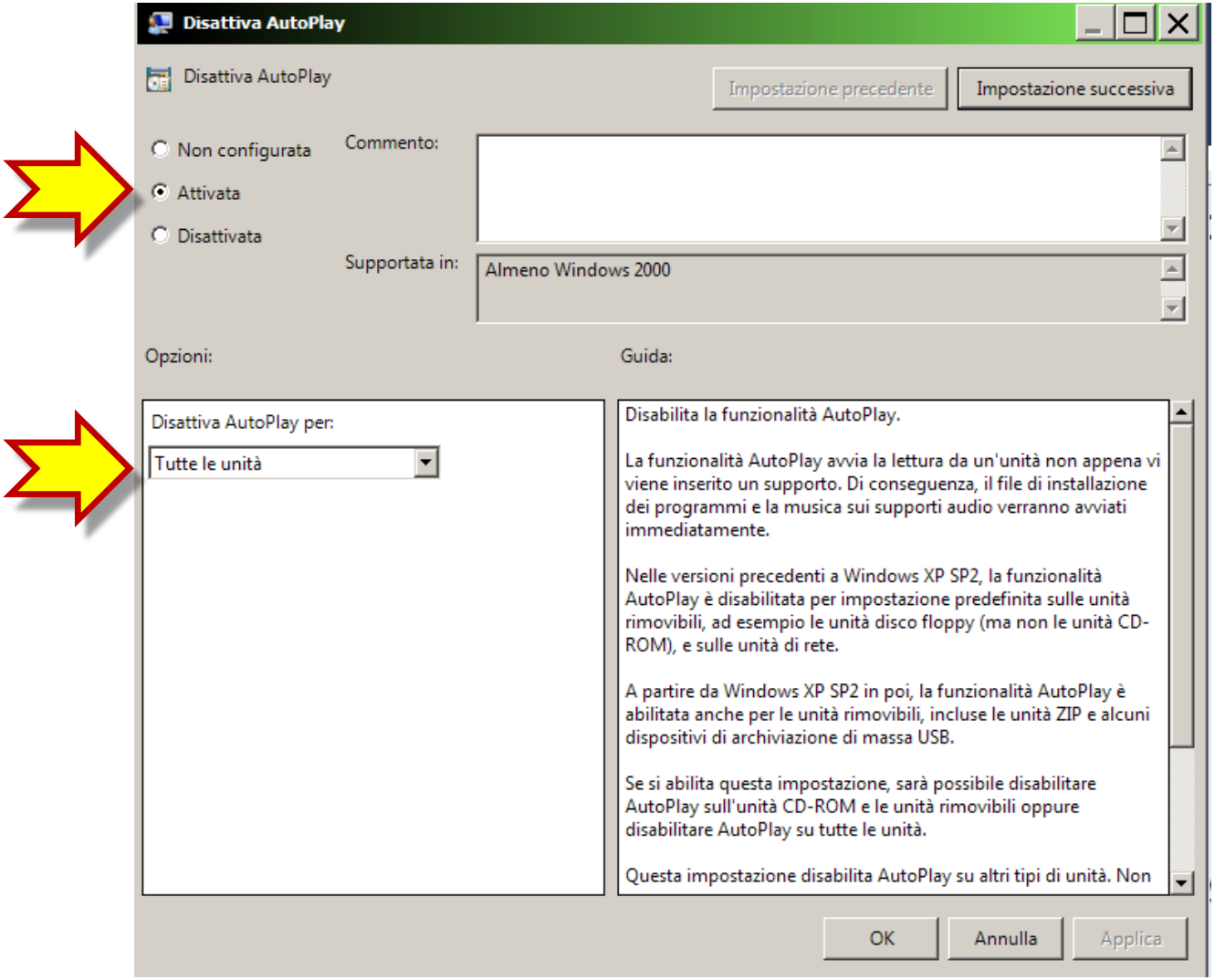
- menù Start > Esegui (oppure win+r),
- scrivi gpedit.msc e premi invio
- compare l'*Editor Criteri di gruppo locali*
- Vai a Configurazione computer >
  modelli amministrativi >
  componenti di windows >
  criteri AutoPlay

voce "disattiva autoplay": porre su 'attivata' e scegliere tutte le unità

# autorun


Editor Criteri di gruppo locali
File
Azione
Visualizza
?
Criteri Computer locale
Configurazione computer
Impostazioni del software
Impostazioni di Windows
Modelli amministrativi
Componenti di Windows
Pannello di controllo
Rete
Sistema
Stampanti
Tutte le impostazioni
Configurazione utente
Impostazioni del software
Impostazioni di Windows
Modelli amministrativi
Componenti di Windows
Selezionare un elemento per visualizzarne la descrizione.
Impostazione
Analisi dell'affidabilità Windows
Analisi utilizzo software Windows
Assistenza online
Backup
Biometria
Calendario di Windows
Centro PC portatile Windows
Centro sicurezza PC
Cerca
Compatibilità tra applicazioni
Criteri AutoPlay
Crittografia unità BitLocker
Esplora giochi
Esplora risorse
Feed RSS
Gadget per il desktop
Gestione finestre desktop
Gestione remota Windows
Gestione risorse di sistema Windows
Gruppo Home
Impostazioni presentazioni
Inoltro eventi
Esteso
Standard


Editor Criteri di gruppo locali
File
Azione
Visualizza
?
Criteri Computer locale
Configurazione computer
Impostazioni del software
Impostazioni di Windows
Modelli amministrativi
Componenti di Windows
Analisi dell'affidabilità Windows
Analisi utilizzo software Windows
Assistenza online
Backup
Biometria
Calendario di Windows
Centro PC portatile Windows
Centro sicurezza PC
Cerca
Compatibilità tra applicazioni
Criteri AutoPlay
Crittografia unità BitLocker
Esplora giochi
Esplora risorse
Feed RSS
Gadget per il desktop
Gestione finestre desktop
Gestione remota Windows
Gestione risorse di sistema Windov
Gruppo Home
Impostazioni presentazioni
Inoltro eventi
Criteri AutoPlay
Disattiva AutoPlay
Modifica impostazione criterio
Requisiti:
Almeno Windows 2000
Descrizione:
Disabilita la funzionalità AutoPlay.
La funzionalità AutoPlay avvia la lettura da un'unità non appena v viene inserito un supporto. Di conseguenza, il file di installazi programmi e la musica sui sup audio verranno avviati immediatamente.
Nelle versioni precedenti a Windows XP SP2, la funzionalità AutoPlay è disabilitata per impostazione predefinita sulle unità rimovibili, ad esempio le unità disco floppy (ma non le unità CD-ROM), e sulle unità di rete.
A partire da Windows XP SP2 in poi, la funzionalità AutoPlay è abilitata anche per le unità rimovibili, incluse le unità ZIP e alcuni dispositivi di archiviazione di massa USB.
Impostazione
Disattiva AutoPlay
Non selezionare la casella di controllo Esegui sempre ques
iva AutoPlay per dispositivi non di volume
rtamento predefinito di esecuzione automatica
Esteso
Standard
4 impostazione/i


Disattiva AutoPlay
Disattiva AutoPlay
Impostazione precedente
Impostazione successiva
Non configurata
Attivata
Disattivata
Commento:
Supportata in:
Almeno Windows 2000
Opzioni:
Guida:
Disattiva AutoPlay per:
Tutte le unità
Disabilita la funzionalità AutoPlay.
La funzionalità AutoPlay avvia la lettura da un'unità non appena vi viene inserito un supporto. Di conseguenza, il file di installazione dei programmi e la musica sui supporti audio verranno avviati immediatamente.
Nelle versioni precedenti a Windows XP SP2, la funzionalità AutoPlay è disabilitata per impostazione predefinita sulle unità rimovibili, ad esempio le unità disco floppy (ma non le unità CD-ROM), e sulle unità di rete.
A partire da Windows XP SP2 in poi, la funzionalità AutoPlay è abilitata anche per le unità rimovibili, incluse le unità ZIP e alcuni dispositivi di archiviazione di massa USB.
Se si abilita questa impostazione, sarà possibile disabilitare AutoPlay sull'unità CD-ROM e le unità rimovibili oppure disabilitare AutoPlay su tutte le unità.
Questa impostazione disabilita AutoPlay su altri tipi di unità. Non
OK
Annulla
Applica

# regole spicciole

- bloccare il PC quando ci assenta
- usare password serie (v. modulo 3.4)
- non usare account amministrativi (v. modulo 3.6)
- non far usare il proprio PC da terzi

# installazione di windows

<u>subito</u> installare:

- USB guard
- antivirus
- antispyware
- antimalware
- firewall
- (x)crypt

- browser (ev. TOR, no chrome)
- noscript
- AD blocker
- cambiare motore di ricerca
- impostazioni cronologia
- impostazioni aggiornamenti

*meglio se da CD*

# *(segue)*

- chiusura porte
- disinstallare / bloccare aggiornamenti ~~spia~~ sospetti
- far cancellare il file di swap in chiusura
- eliminare *hiberfil.sys*
- disabilitare punti di ripristino
- creare seconda partizione per i dati e
- **spostare il desktop**

il penultimo stadio di hardening di un computer è renderlo

**AIR-GAPPED**

(cioè isolato da tutte le reti, con tutte le porte bloccate, ecc.)

ma non sempre è fattibile

# *M4.2* – Sistemi informatici integrati e misure di sicurezza

## *Backup – I parte*

# BACKUP

Protezione essenziale

e

nuovo pericolo

# Il backup protegge da:

- Modifiche e cancellazioni accidentali
  (in generale, errori umani)
- aggiornamenti e nuove versioni del software
- attacchi a SYSKEY
- Minacce varie

e costituisce il substrato per il **Disaster Recovery**

# Cause di perdita di dati

## Per utenti avveduti:

1. Guasti
2. Furti
3. Calamità
4. Virus & malware

# Cause di perdita di dati

**Per utenti avveduti:**

1. Guasti
2. Furti
3. Calamità
4. Virus & malware

**Per utenti *inesperti:***

1. Virus & malware
2. Furti
3. Calamità
4. Guasti

# guasti

www.backblaze.com/blog/2018-hard-drive-failire-rates/

# furti

verte: «Napoli / città di ladri / attenzione» e prosegue indicando dettagliatamente come e dove guardarsi dai napoletani.

# rimedi

- Backup preventivo (prima che accada il disastro)
- Salvataggio automatico
- RAID

*…tutto per evitare il*

Recupero di emergenza

# Recupero di emergenza

I *tentativi* di recuperare i dati da un hard disk guasto devono essere svolti in camera bianca, da personale qualificato (= $$$)

Non sempre si hanno i risultati sperati

regola di base

**!**

**non deve mai esistere**

**una sola copia**

**di un file**

# GDPR e backup

**Articolo 32 – Sicurezza del trattamento**

*1) Tenuto conto dello stato dell'arte e dei costi di attuazione (...)*

- *a) la pseudonimizzazione e la cifratura dei dati personali;*
- *b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;*
- *c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;*
- *d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

# GDPR e backup

Il GDPR crea grossi problemi al backup:

Diritto all'oblio

it.quora.com/Come-la-mettiamo-con-i-backup-nel-contesto-del-GDPR-Cancellare-i-dati-personali-dai-backup-passati-non-%C3%A8-compatibile-col-concetto-stesso-di-backup

www.cybersecurity360.it/legal/privacy-dati-personali/gdpr-e-data-retention-conservazione-dati-policy-e-linee-guida-per-farla-bene/

# Duplicazione e sincronizzazione

***Duplicazione**:* creare una nuova copia (che è un nuovo originale)

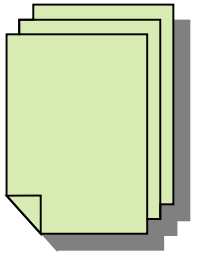
***Sincronizzazione**:*

copiare i file nuovi

sostituire quelli cambiati

eliminare quelli cancellati

# versioning

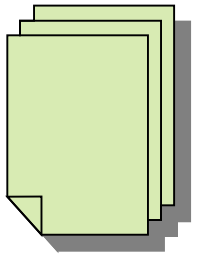


Conservare le ultime *n* versioni dei file

Il numero di copie da mantenere dipende da:

- Tipo dei dati
- Norme
- Abitudini aziendali / personali

# versioning



Report_001.rtf
Report_002.rtf
Report_003.rtf
...

Tabella_2018.03.04.odf
Tabella_2018.05.11.odf
Tabella_2018.10.07.odf
...

# supporti

Ovvero: dove conservare i backup?

- Nastri
- Dischi
- Cloud

# nastri

# nastri


TDK
DC 6250
FUJIFILM
DG4-150


hp
LTO-5 Ultrium RW
DATA CARTRIDGE
3TB*

# nastri - *library*


# nastri

**Pro:**

- Economia
- Diffusione
- ingombro

**Contro:**

- Lentezza
- Stoccaggio

# dischi

**Pro:**

- velocità

**Contro:**

- costo
- ingombro online

# cloud

Memorizzare le copie su un server remoto

(Magari a distanza geografica tale da superare anche eventi catastrofici)

# cloud

**Pro:**

- Separazione fisica
- Semplicità
- Mancanza di infrastruttura locale

**Contro:**

- Costi
- Necessità della connessione
- Dati in mano a terzi (in quale Paese?)

Recovery Time Objective (RTO)

e

Recovery Point Objective (RPO)

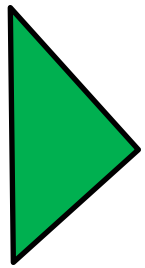
# *M4.2* – Sistemi informatici integrati e misure di sicurezza

## *Backup – II parte*

*Dott. R. Grieco*

# Backup - tipologie

- Full (completo)
- Differenziale
- Incrementale



# Backup - tipologie

- Full (completo)

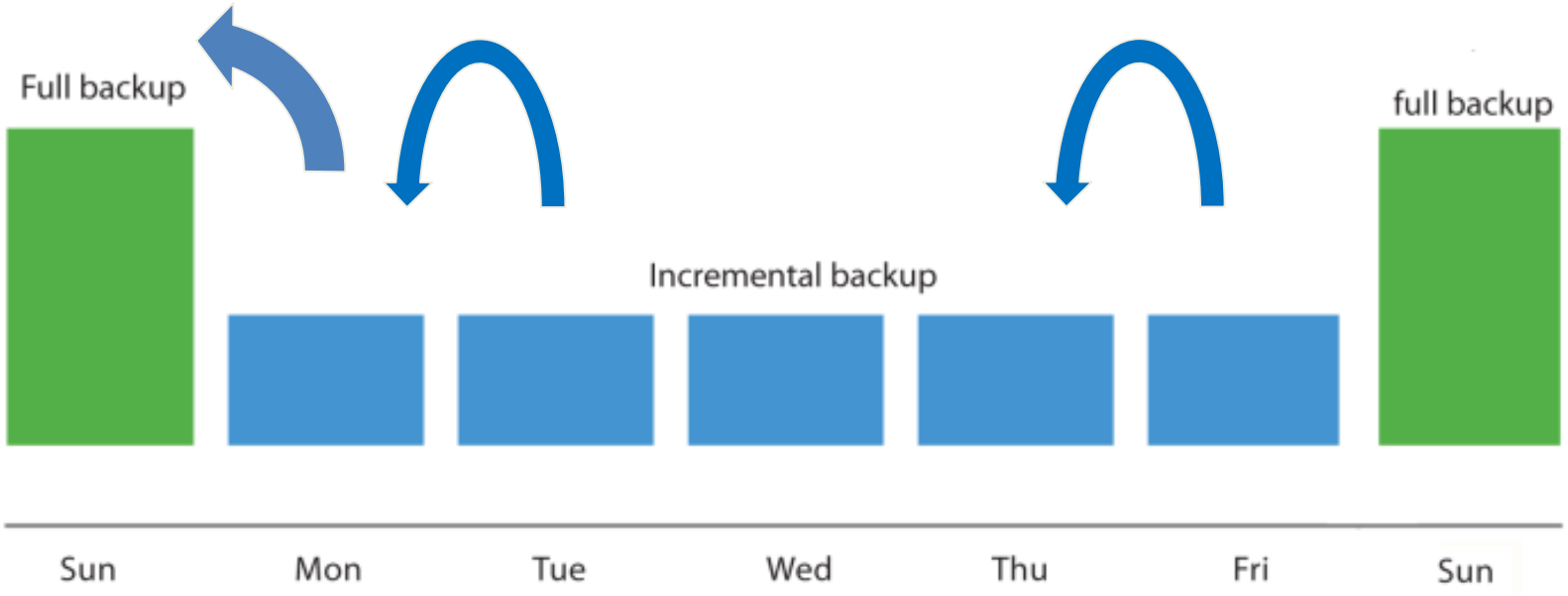
  Si salvano tutti i file

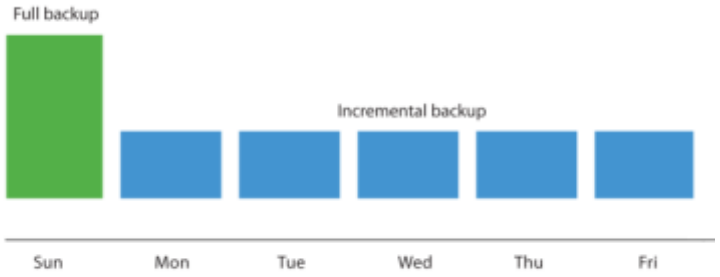
- Differenziale

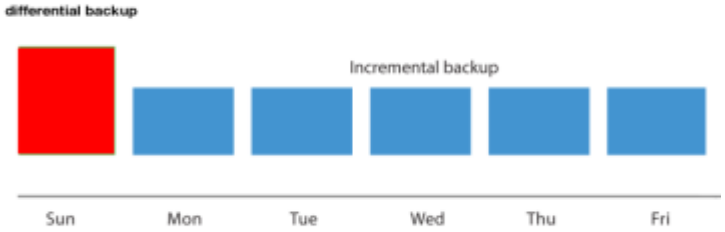
  Si salvano i file cambiati dall'ultimo *full*

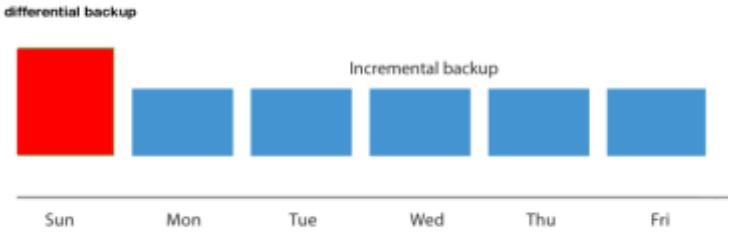
- Incrementale

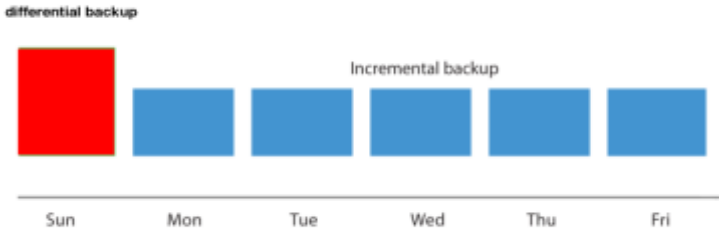
  Si salvano i file cambiati dall'ultimo backup


Full backup
Incremental backup
full backup
Sun
Mon
Tue
Wed
Thu
Fri
Sun


Full backup
Incremental backup
Sun
Mon
Tue
Wed
Thu
Fri


differential backup
Incremental backup
Sun
Mon
Tue
Wed
Thu
Fri


differential backup
Incremental backup
Sun
Mon
Tue
Wed
Thu
Fri


differential backup
Incremental backup
Sun
Mon
Tue
Wed
Thu
Fri

# RAID

Redundant Array of Inexpensive Disks

ora

Redundant Array of *Independent* Disks

# RAID

Utilizza più dischi insieme per migliorare, rispetto a un disco singolo:

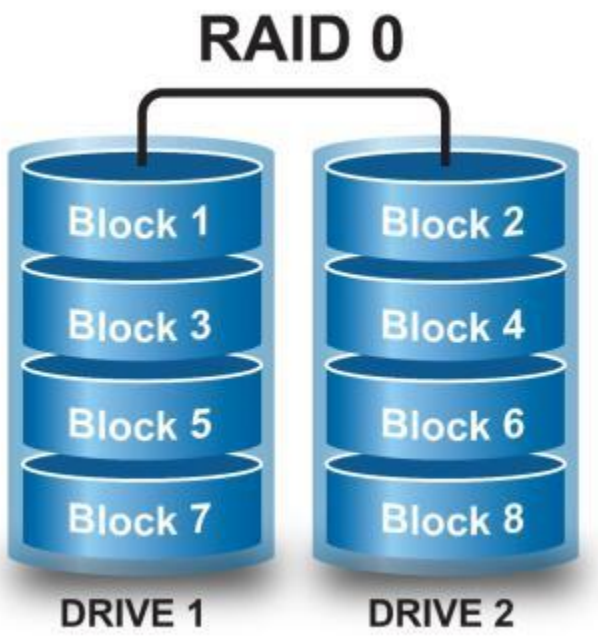
- Velocità
- Affidabilità
- Capacità
- un mix delle precedenti

# RAID

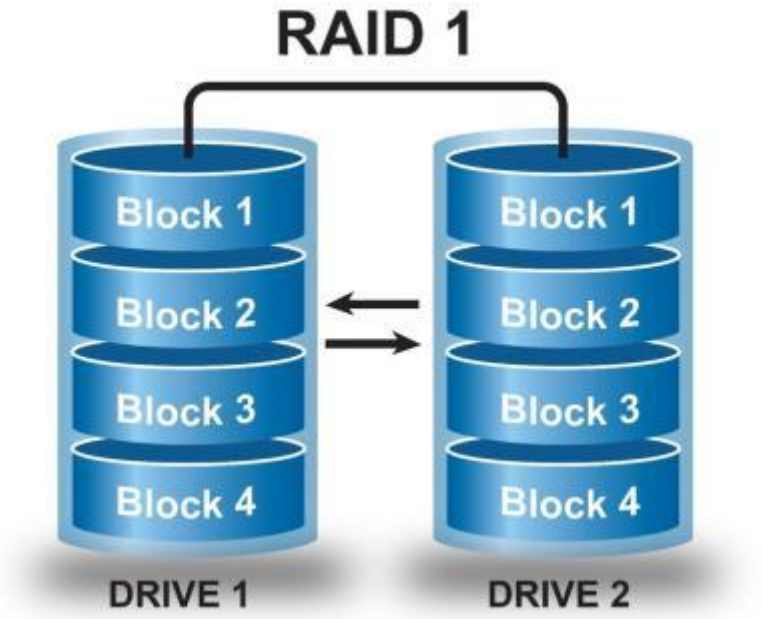
Il concetto base è che sui dati si possono effettuare delle **operazioni**

I risultati delle operazioni permettono di costruire della ridondanza che torna utile in caso di guasto

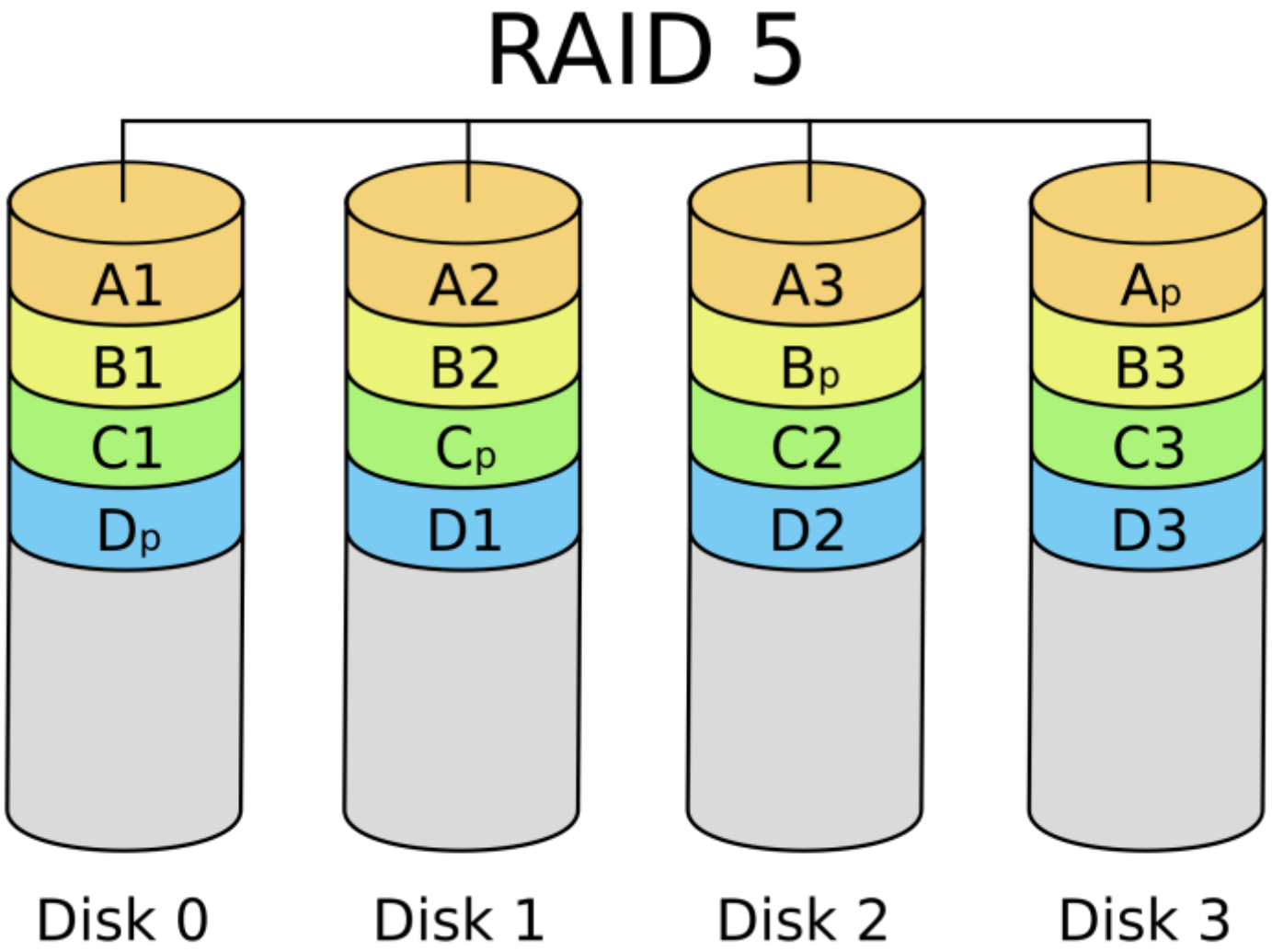
# Livelli RAID




striping




mirroring


RAID 5
A1
B1
C1
Dp
A2
B2
Cp
D1
A3
Bp
C2
D2
Ap
B3
C3
D3
Disk 0
Disk 1
Disk 2
Disk 3

**Raid 0** *(striping)*: veloce, capiente, pericolosissimo

**Raid 1** *(mirror):* affidabile ma sprecone

**Raid 5**: via di mezzo

**Raid 6**: come raid 5 ma ancora più affidabile

nei RAID 5 e superiori si possono impostare uno o più dischi come hot spare (riserva)

sostituiscono subito e automaticamente il disco guasto

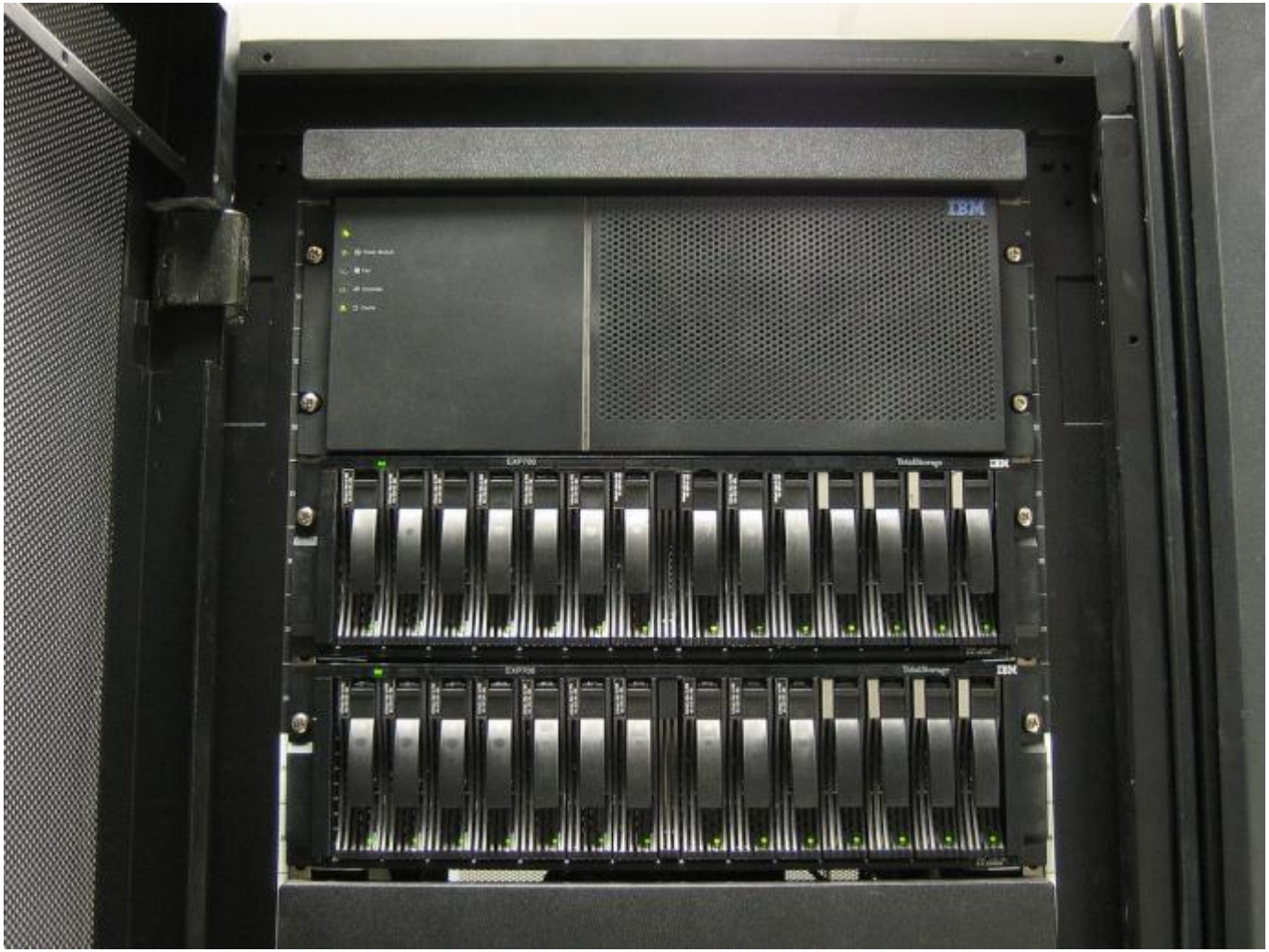
anche di notte e nei festivi

## RAID software

N dischi collegati normalmente, la ridondanza è a cura del Sistema Operativo

## RAID hardware

N dischi in un dispositivo apposito, la ridondanza è a cura dell'apparecchio.


IBM

# Storage Area Network

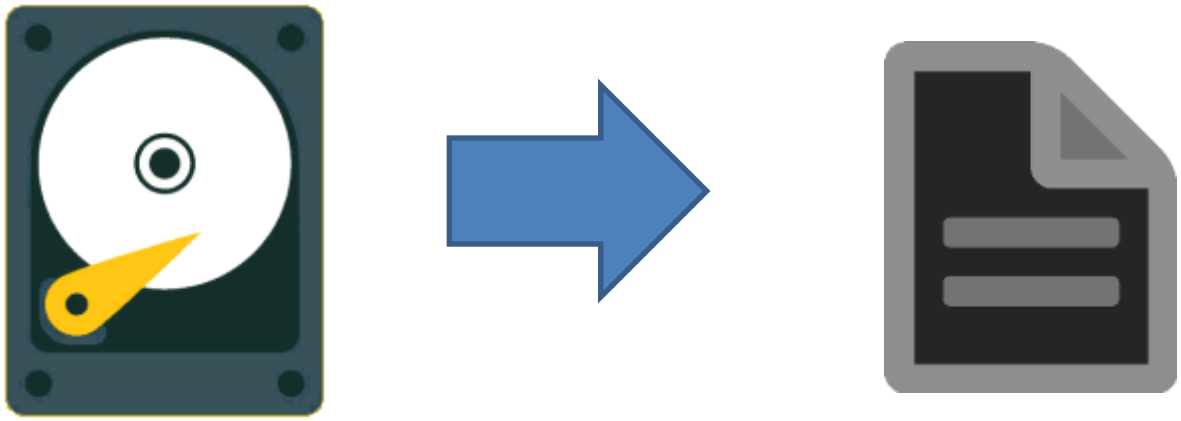
# Raid domestico / SOHO

# Raid domestico / soho

# RAID portatile


# *Immagine* del S. O.

copia integrale di un disco (tipicamente c: o quello di sistema) salvata su un file

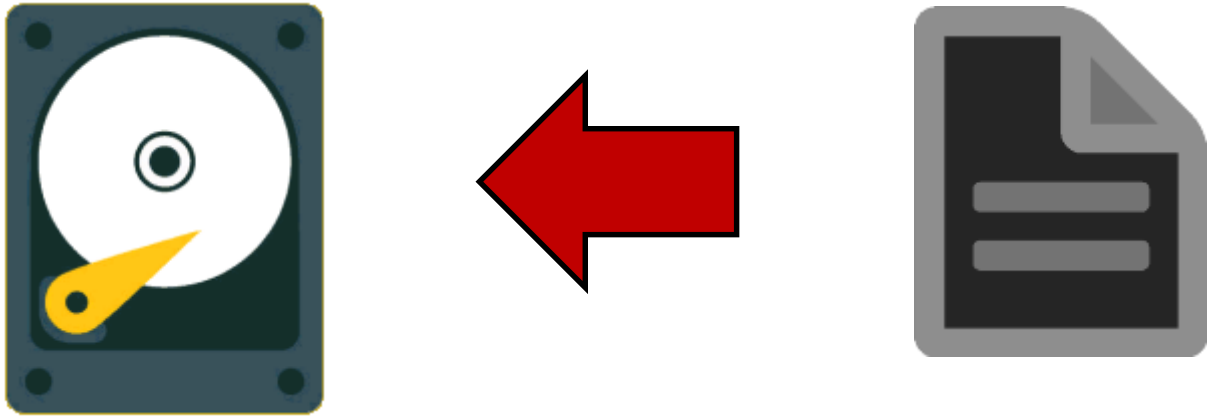


# *Immagine* del S. O.

permette di ritornare facilmente a uno stato precedente per ovviare a un guaio (virus, malware, aggiornamento sballato...)

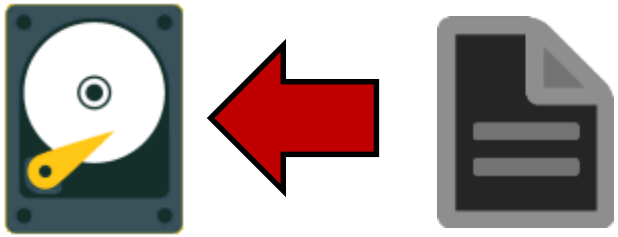
si usa anche per installare tante copie di un sistema operativo su un parco macchine esteso

# Restore (ripristino)



Dopo il restore, il sistema sarà nello stesso stato in cui era al momento in cui è stata creata l'immagine (che può essere 1 anno, 1 mese o 1 giorno fa)...

# Restore (ripristino)



Occorre solo fare attenzione ai dati che eventualmente vengono salvati sulla partizione / disco C: (cattiva abitudine)

In windows il pericolo maggiore è il **desktop**

# *Immagine* del S. O.

## programmi free:

Macrium Reflect

AOMEI Backupper

Ghost

Clonezilla

Ricordarsi di **togliere** la password del sistema operativo di cui si fa l'immagine

...oppure memorizzarla in modo sicuro

# Aggiornamenti

- possono riguardare il sistema operativo o i programmi applicativi
- è successo (e la frequenza aumenta) che un aggiornamento crei nuovi problemi o ne risolva alcuni e ne crei altri
- (patch per Spectre e Meltdown)

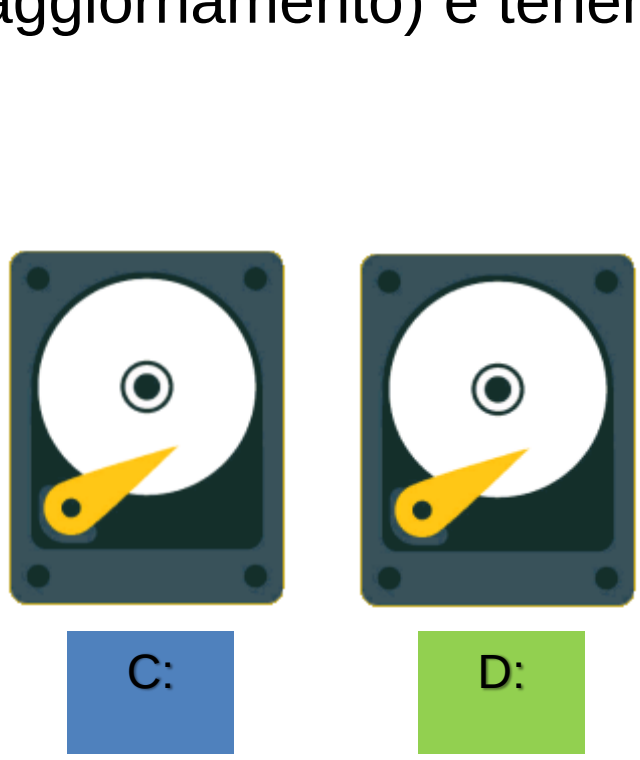
"Windows 10, attenti all'aggiornamento: potrebbe cancellare i documenti"

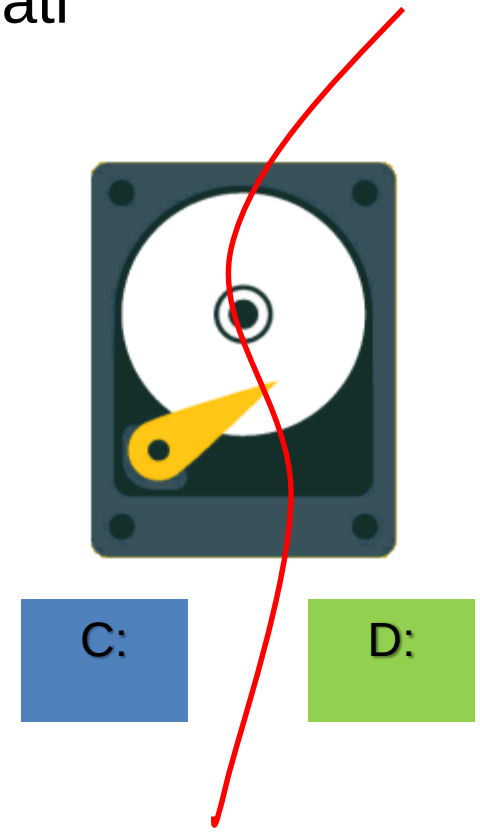
www.zeusnews.it/n.php?c=26746


"Windows 10: l'update cancella i file, distribuzione fermata"

www.tomshw.it/windows-10-update-cancella-file-distribuzione-fermata-98159

si può rimediare facendo l'immagine del S.O. con frequenza opportuna (al limite subito prima di installare un aggiornamento) e tenendo separati i dati



# *M4.2* – Sistemi informatici integrati e misure di sicurezza

## *Cifratura – I parte*

*Dott. R. Grieco*

# CIFRATURA

# esempi classici

- Enigma
- Cifrario Beale
- Memorizzazione delle password
- DRM
- telefoni cellulari
- DVD e Blu-Ray
- Abbonamenti TV a pagamento

# storia

- cifrario di cesare (sostituzione monoalfabetica)
- cifrario di Vigenère (sostituzione polialfabetica)
- cifrario di Vernam ("cifrario perfetto", chiave lunga quanto il testo)

# esercizio

decriptare:

LXVKJCCR BXUX UN PDNAAN LQN YDXR ERWLNAN...
YANYJAJCR YNA UN PDNAAN LQN MNER LXVKJCCNAN
-MNUUJ PDNAAJ, LJAU EXW LUJDBNFRCI

# esercizio

COMBATTI SOLO LE GUERRE CHE PUOI VINCERE...
PREPARATI PER LE GUERRE CHE DEVI COMBATTERE

-DELLA GUERRA, CARL VON CLAUSEWITZ

# fiducia

## des / aes

Nel 1977 il National Bureau of Standards chiese un sistema per proteggere le transazioni commerciali (URSS)

Fu introdotto il DES, ma la chiave fu portata dagli iniziali 64 a 56bit

già nel 1998 il DES-Challenge mostrò che il DES poteva essere violato in pochi giorni

# fiducia

## Exclusive: NSA encryption plan for 'internet of things' rejected by international body

*An attempt by the U.S. National Security Agency (NSA) to set two types of encryption as global standards suffered a major setback on Tuesday, after online security experts from countries including U.S. allies voted against the plan, for use on the "internet of things."*

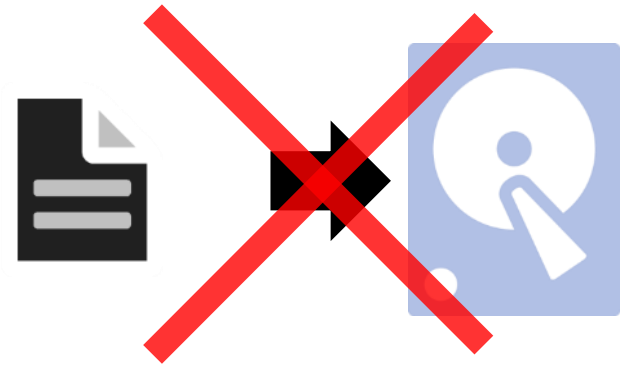
www.wikitribune.com/article/67004/

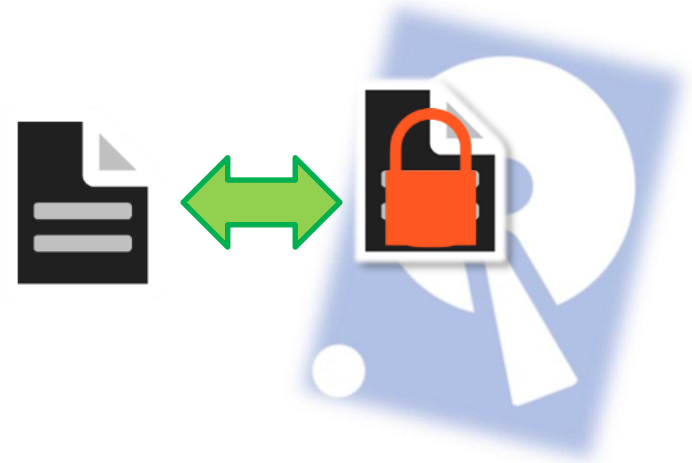
# Software per la Cifratura

- **Free OTFE** → LibreCrypt
- **PGP**
- **Truecrypt** → CipherShed, tc-play / ZuluCrypt, Veracrypt
- **DiskCrypt, AxCrypt, ...**
- **Linux Unified Key Setup (LUKS)**

# On-the-fly encryption

- i file non vengono mai scritti in chiaro su disco
- cifratura e decifratura avvengono sempre direttamente tra RAM e archivio criptato





# 1 - Free OTFE

- 2004
- FreeOTFE4PDA (windows mobile)

- Sarah Dean non dà notizie dal 2011, il sito è finito in mano a estranei e il programma si trova solo su SourceForge

# 2 - PGP (pretty good privacy)

creato nel 1991 come software proprietario

le sue specifiche sono state raccolte dall'IETF e nasce OpenPGP

Nel 1993 Zimmermann fu accusato di esportazione di armi dal governo USA

con l'allentamento delle restrizioni PGP l'incriminazione è stata archiviata

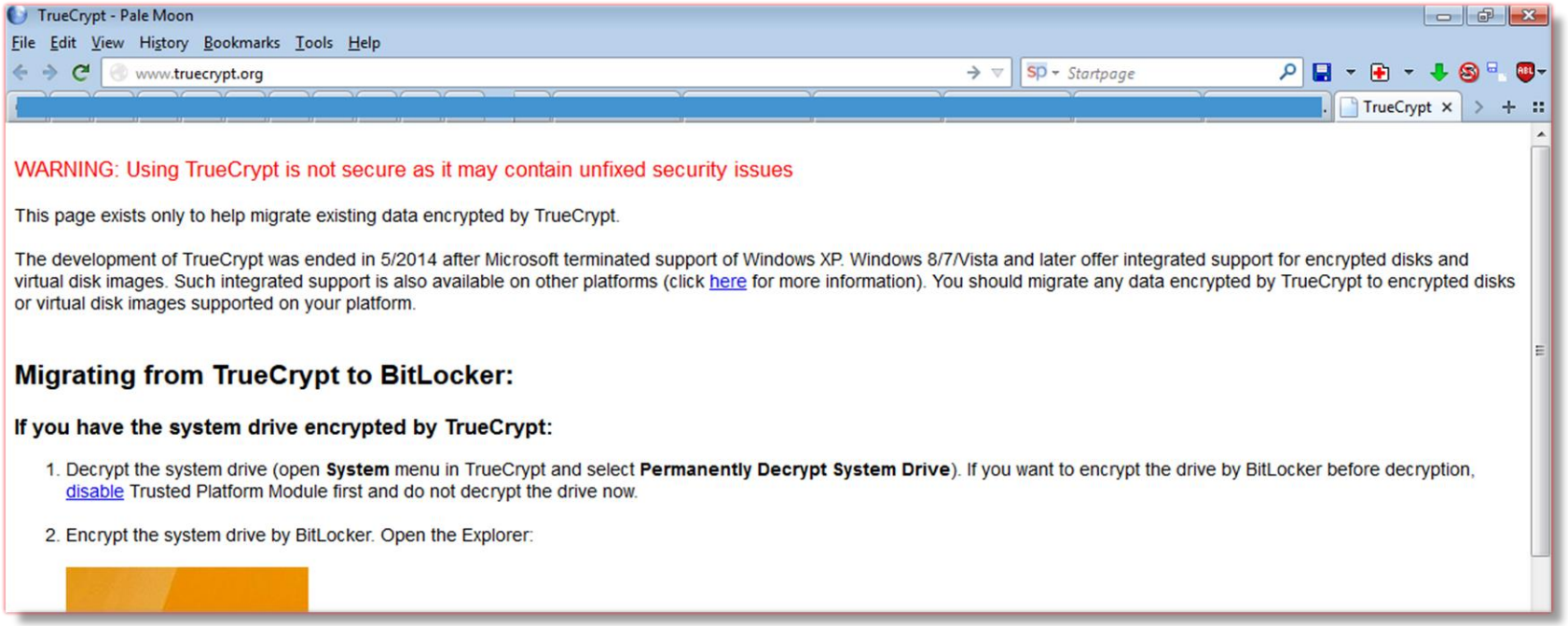
brevettato solo negli USA (2 versioni)

PZ in una intervista dichiara pressioni per inserire una backdoor e non dare il sorgente

Phil Zimmermann

# 3 - Truecrypt

- la versione 7.1a è l'ultima rilasciata
- il 28 maggio 2014 è stata annunciata la cessazione:



# Truecrypt

il programma è stato sottoposto a 2 audit di sicurezza

www.schneier.com/blog/archives/2015/04/truecrypt_secur.html

il suo successore è considerato VeraCrypt,

che tra l'altro ha corretto i piccoli errori trovati negli audit

# Cassandra Crossing/ Un tranquillo weekend di TrueCrypt

La confusione è calata su TrueCrypt, ma non è opportuno farsi prendere dal panico. Le alternative esistono, e sono praticabili

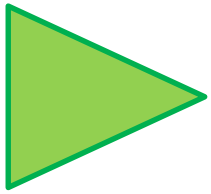
www.punto-informatico.it/cassandra-crossing-un-tranquillo-weekend-di-truecrypt/

# Funzionamento

il software di cifratura permette di creare un archivio criptato sotto forma di:

File / Partizione / Disco;

all'archivio ("volume") viene assegnata una *passphrase*



- inserendo la passphrase il volume si "apre",
- compare una nuova lettera di unità ed
- è possibile lavorare sui file come se fosse un hard disk o una memoria USB

- al termine si chiude il volume, la lettera scompare e il contenuto non è più accessibile

altro vantaggio:

non è necessario preoccuparsi della cancellazione definitiva in un volume cifrato. E' automatica.

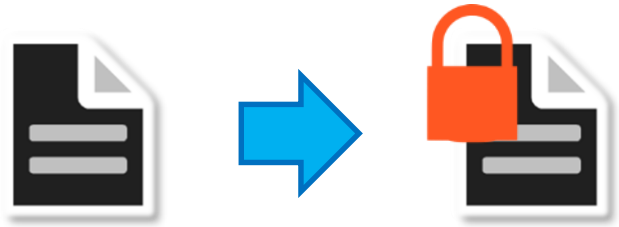
(tech: lo spazio occupato da un file cancellato viene riempito con contenuto pseudocasuale per mantenere la sicurezza)

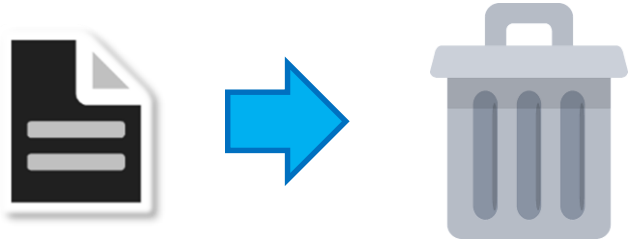
# *M4.2* – Sistemi informatici integrati e misure di sicurezza

## *Cifratura – II parte*

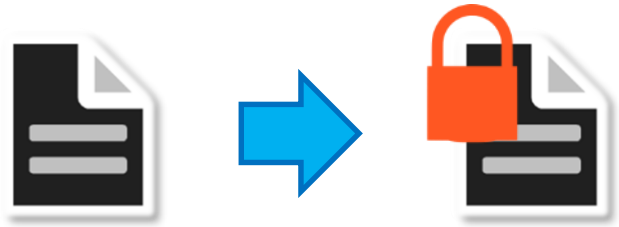
*Dott. R. Grieco*

# cifratura base

1. 

2. 

# cifratura base

1. 

2. 

# v. modulo 4.6

(cancellazione sicura)

# trasporto

perfino gli agenti di CIA, FBI e NSA dimenticano i portatili in taxi...

...perchè non può capitare a te?

# suggerimenti

- criptare tutto il disco
- eliminare l'ibernazione
- portare in giro il PC spento
- solite regole per la password

# Password Hacking

- intercettare la password
- studiare le variazioni
- accesso fisico al PC
- attacco brute-force

- intercettare la password
- studiare le variazioni

evitare che il nemico abbia copie successive dell'archivio

- accesso fisico al PC
- attacco brute-force

# Ulteriori difese

- Keyfiles
- Pre-boot authentication
- Plausible Deniabillity
- sistema operativo *nascosto*

# SED (Self-Encrypting Drives)

Hard disk con incorporato il sistema di cifratura

# SED (Self-Encrypting Drives)

## La falla negli SSD che vanifica completamente la crittografia

*Coinvolti i modelli più popolari di Crucial e Samsung.*

www.zeusnews.it/n.php?c=26818

## Bug nella crittografia hardware dei dischi SSD Samsung e Crucial

www.securityinfo.it/2018/11/06/bug-nella-crittografia-hardware-dei-dischi-ssd-samsung-e-crucial/

# Crypt – hardware


64GB


CORSAIR


64GB

# M4.3 La Legge 231/01 e i reati informatici

# M4.4 Whistleblowing e segnalazioni all'Organismo di Vigilanza

Avv. Ida Tascone

# Il pragmatismo

Il pragmatismo che caratterizza il decreto è un elemento decisivo, che le aziende devono assumere per affrontare ed evitare la responsabilità da reato

# Il pragmatismo

Assumendo questa definizione del pragmatismo si può ribadire che l'unica verità rilevante della responsabilità da reato delle aziende coincide con le azioni da organizzare per evitarla.

# Il pragmatismo

Più che le definizioni, sono importanti le **azioni** e gli **esempi**: in tal senso diventa naturale e doveroso interpretare tutto il "sistema 231" come un insieme giuridicamente caratterizzato da pratiche organizzative all'interno degli enti e delle aziende.

# Cass. Pen. SU n. 26654/2008

Sezioni Unite della Corte di Cassazione nella sentenza n. 26654 del 2008, hanno affermato che il D.Lgs. n.231/2001 è

"l'epilogo di un lungo cammino volto a contrastare il fenomeno della criminalità d'impresa, attraverso il superamento del principio, insito nella tradizione giuridica nazionale, ***societas delinquere non potest*** e nella prospettiva di omogeneizzare la normativa interna a quella internazionale di matrice prevalentemente anglosassone, ispirata al c.d. **pragmatismo giuridico**".

# D.lgs. 231/2001

Il D.Lgs. n. 231/2001 stabilisce che l'azienda italiana che vuole evitare la responsabilità da reato deve, fra le altre cose, adottare un **Modello Organizzativo e Gestionale (MOG)** di prevenzione dei reati: un insieme vero e proprio di precetti e procedure comportamentali, che può permettere l'esclusione della responsabilità o una forte diminuzione della pena.

# D. Lgs. 8 giugno 2001 n. 231: la responsabilità penale-amministrativa degli enti.

**D.Lgs. 231/01 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica**

*(Gazzetta Ufficiale n. 140 del 19 giugno 2001)*

**Art. 1:**

Le disposizioni si applicano agli "enti" forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica

Non si applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale

# Casi più significativi di applicazione della responsabilità amministrativa da reato

- Gruppi di società;
- Società per azioni, anche unipersonali;
- Società in accomandita per azioni;
- Società a responsabilità limitata, anche unipersonali;
- Società in nome collettivo;
- Società semplici;
- Società in accomandita semplice;
- Società cooperative;
- Società mutue assicurative;

# Casi più significativi di applicazione della responsabilità amministrativa da reato

- Società per azioni con partecipazione dello Stato o degli enti pubblici;
- Società per azioni di interesse nazionale;
- Società previste da leggi speciali: società di intermediazione finanziaria, società di investimento a capitale variabile e gestione di fondi comuni di investimento, società di revisione, intermediari finanziari, etc.;
- Consorzi;
- Società irregolari;
- Società di fatto;
- Enti pubblici economici.

# A quali soggetti non si applicano le disposizione del D.Lgs. 231/01?

## Casi più significativi di esclusione:

- Stato;
- Regioni;
- Province;
- Comuni;
- Altri enti pubblici territoriali;
- Enti pubblici non economici;
- A.T.I.: in caso di reato commesso nell'ambito operativo delle Associazioni Temporanee di Imprese da una delle imprese associate ne risponde solo quest'ultima e non l'intero raggruppamento, perché l'Associazione Temporanea di Impresa non realizza un soggetto giuridico che si distingue dalle società che la costituiscono.

# PRESUPPOSTI PER LA RESPONSABILITA' EX D. Lgs. 231/01:

1. Commissione di un reato previsto dal decreto 231;
2. Commissione del reato da parte di un soggetto in posizione "apicale" o "subordinata";
3. Interesse o vantaggio dell'ente derivante dalla commissione del reato.

in sostanza si afferma che:

*Gli Enti sono ritenuti responsabili per i reati commessi nel loro interesse e/o vantaggio da "persone" che al loro interno rivestono ruoli di responsabilità e direzione.*

L'ente non risponde se le "persone" hanno agito nell'interesse esclusivo proprio o di terzi

# 1.ELENCO DEI REATI PRESUPPOSTO

– tipologia in continua evoluzione

• ***Reati contro la Pubblica Amministrazione***

✓Concussione, corruzione

✓Indebita percezione di erogazioni a danno dello Stato o di altro Ente pubblico

✓Frode informatica a danni dello Stato o di altro Ente pubblico

• ***Reati societari***

✓Ipotesi di falsità (false comunicazioni sociali e false comunicazioni sociali in danno della Società, dei soci e dei creditori)

✓Fattispecie poste a tutela del capitale sociale (indebita restituzione dei conferimenti; illegale ripartizione degli utili e delle riserve; illecite operazioni sulle azioni o quote sociali o della Società controllante; operazioni in pregiudizio dei creditori; omessa comunicazione del conflitto di interessi; formazione fittizia del capitale)

✓Fattispecie poste a tutela del regolare funzionamento della Società (impedito controllo; illecita influenza sull'assemblea)

• ***Reati informatici e trattamento illecito di dati***

✓ Falsità in documenti informatici

✓ Accesso abusivo ad un sistema informatico o telematico

✓ frode informatica del soggetto che presta servizi di certificazione di firma elettronica

# 1.ELENCO DEI REATI PRESUPPOSTO

– tipologia in continua evoluzione

- ***Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita***

- ***Reati in violazione della normativa sulla salute e sicurezza del lavoro***

✓ Omicidio colposo

✓ Lesioni colpose gravi o gravissime

- ***Delitti contro la fede pubblica***

✓ Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di opere industriali

✓ Introduzione nello Stato e commercio di prodotto con segni falsi

# 1.ELENCO DEI REATI PRESUPPOSTO

– tipologia in continua evoluzione

- ***Reati transnazionali***
- ***Delitti di criminalità organizzata***
- ***Delitti contro la personalità individuale***
- ***Pratiche di mutilazione degli organi genitali femminili***
- ***Delitti di terrorismo***
- ***Market Abuse***

✓ Abuso di informazioni privilegiate

✓ Manipolazioni di mercato

# 1.ELENCO DEI REATI PRESUPPOSTO

– tipologia in continua evoluzione

- ***Delitti contro l'industria ed il commercio ed in materia di violazione del diritto d'autore***

✓ Illecita concorrenza

✓ Fabbricazione e commercio di beni usurpando titoli di proprietà industriale

✓ Protezione del diritto d'autore e di altri connessi al suo esercizio

- ***Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria***

- ***Reati ambientali***

Il D.Lgs. 121 del 07/07/201, ha introdotto, con efficacia dal 16 agosto 2011, tra i reati presupposto diversi reati a tutela dell'ambiente aventi ad oggetto la gestione dei rifiuti, degli scarichi industriali, la bonifica di siti, l'inquinamento in atmosfera, l'inquinamento navale e la tutela di specie animali e vegetali in via di estinzione.

# CRIMINI INFORMATICI: Legge 48/08

La Legge 18 marzo 2008, n. 48, di ratifica alla Convenzione del Consiglio d'Europa sulla Criminalità informatica (cd. Convenzione di Budapest), ha determinato le seguenti modifiche:

Adeguamento della normativa del codice penale e del codice di rito in tema di reati informatici

(dopo quasi quindici anni di applicazione della legge 547/1993, che rappresentò il primo intervento organico in materia).

Introduzione nel D.lgs. 231/01 del nuovo art. 24 *bis*, che estende la responsabilità amministrativa delle persone giuridiche anche ai c.d. reati di Criminalità Informatica.

Integrazione, dal punto di vista procedurale, delle modalità di accesso da parte delle forze dell'ordine ai dati di traffico conservati dagli operatori di comunicazione elettronica ai sensi dell'art. 132 del Codice della privacy (D.Lgs.196/03).

# CRIMINI INFORMATICI: L'art. 24 bis D.lgs. 231/01


***Art. 615- ter*:**

Accesso abusivo ad un sistema informatico o telematico

***Art. 615- quater*:**

Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici

***Art. 615- quinquies*:**

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informativo o telematico

***Art. 617- quater*:**

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

***Art. 617- quinquies*:**

Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche

***Art. 635- bis:***

Danneggiamento di informazioni, dati e programmi informatici

***Art. 635- ter:***

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

***Art. 635- quater:***

Danneggiamento di sistemi informatici o telematici

***Art. 635- quinquies:***

Danneggiamento di sistemi informatici o telematici di pubblica utilità

***Art. 640- quinquies:***

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

***Art. 491- bis:***

Falsità di documenti informatici

# CRIMINI INFORMATICI: L'art. 25 D.lgs. 231/01

**Prima dell'entrata in vigore della Legge 48/08, già l' art. 25 D.lgs. 231/01 aveva previsto l'estensione della responsabilità amministrativa delle persone giuridiche alle seguenti fattispecie di reato, che prevedono l'utilizzo di sistemi informatici:**

*Art. 640-ter:*

Frode informatica in danno dello Stato o di altro Ente Pubblico

*Art. 600-ter e quater:*

Divulgazione, cessione e detenzione di materiale pedopornografico

*Art. 270-ter:*

Fornitura di strumenti di comunicazione in assistenza a gruppi terroristici

# CRIMINI INFORMATICI: modalità di compimento

Con riferimento alle modalità di compimento, i reati possono essere suddivisi nelle seguenti categorie:

- DANNEGGIAMENTO, ACCESSO ABUSIVO, DIFFUSIONE DI VIRUS, MATERIALI E INFORMAZIONI ILLEGALI, ATTRAVERSO:

  **accesso verso l'esterno per mezzo di infrastrutture aziendali**

- FALSITA' IN "DOCUMENTI INFORMATICI", APPLICABILE

  **in caso di utilizzo di "firma digitale" o "firma elettronica avanzata"**

- "FRODE INFORMATICA DEL CERTIFICATORE DI FIRMA ELETTRONICA", APPLICABILE

  **solo in caso che l'azienda sia un "certificatore"**

# Modello di organizzazione e di gestione

## LE SOCIETA' DEVONO ADOTTARE UN SISTEMA DI CONTROLLO PER:

Evitare la commissione di reati informatici per mezzo di infrastrutture proprie

Escludere la responsabilità dell'azienda qualora le misure adottate non abbiano evitato la commissione del reato.

La responsabilità ex. art. 24-bis D.lgs. 231/01 può essere imputata all'azienda anche nelle ipotesi in cui non sia rintracciato l'autore materiale del reato.

*Un indagine svolta da IBM ha rilevato che* ***il 51% delle aziende italiane ritiene che le minacce alla sicurezza aziendale provengano dall'interno delle rispettive organizzazioni.***

## Modello di organizzazione e di gestione

## La prevenzione dei reati informatici deve svolgersi nel rispetto di:

- **Statuto dei Lavoratori L. 300/1970**
- **Legge Privacy L. 196/03**
- **Linee-Guida per l'utilizzo della posta elettronica e di internet del Garante per la protezione dei dati personali.**

Es: Il Codice sulla Privacy, in materia di controllo a distanza, dispone che per quanto attiene il controllo dei dati resta ferma l'applicazione della L. 300/70, che stabilisce il **divieto di uso di impianti audiovisivi o altre apparecchiature per il controllo a distanza dei lavoratori, salvo accordo con i Sindacati.**

Pertanto **l'azienda,** nell'adottare il Modello di Organizzazione Gestione e Controllo, **potrà prevedere l'effettuazione dei controlli sull'attività dei dipendenti svolte mediante l'uso di strumenti informatici solo previo accordo con le Organizzazioni Sindacali.**

# Modelli di organizzazione e di gestione

## Considerazioni

I reati "informatici" sono oggi equiparabili ai reati "tradizionali" (es: violazione del domicilio).
La condanna ex D.Lgs 231/01 della persona giuridica, che ne abbia tratto un vantaggio (interesse), consente di disporre di un patrimonio economico più solido per eventuali richieste di risarcimento.

Lo schema difensivo/accusatorio ex D.Lgs.231/01 basato sull'esistenza di un Modello di controllo:

- comporterà una effettiva prevenzione o un ulteriore onere per le Società più virtuose che si impegneranno ad adottarlo ed efficacemente attuarlo?
- quale giudizio potrà essere formulato in ordine all'efficacia esimente del Modello, la cui bontà appare strettamente connessa all'evoluzione tecnologica informatica?
- elusione delle richieste risarcitorie formulate nei confronti dell'unico centro economico concretamente aggredibile??

# 2. I SOGGETTI AUTORI DEL REATO

- Gli Apicali

- I Subordinati

# Gli Apicali

## Art. 5, lett a) del D.Lgs. 231/01

Persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché persone che esercitano, anche di fatto, la gestione ed il controllo dello stesso.

# Gli Apicali

Sulla base di quanto previsto dal testo del Decreto, da quanto emerso dal dibattito dottrinale e da alcune sentenze, sono sicuramente apicali:

- Amministratore Delegato;
- Presidente del Consiglio di Amministrazione;
- Amministratori S.r.l.;
- Amministratore Unico;
- Membri del Consiglio di gestione
- Consiglieri di Amministrazione con poteri gestionali;
- Direttore generale;
- Delegati dall'apicale;
- Amministratore di fatto o occulto;
- Liquidatori.

# Il potere di fatto..

Il riferimento all'esercizio di fatto delle funzioni di gestione dell'azienda, è fondamentale per comprendere come il "sistema 231" si cali nella realtà concreta dell'impresa per individuarne i soggetti effettivamente responsabili, caso per caso

# I subordinati

## Art. 5, lett b) del D.Lgs. 231/01

Persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

# I subordinati

**Rientrano (o possono rientrare) nei subordinati:**

- I lavoratori subordinati;
- I lavoratori occasionali;
- I lavoratori a progetto;
- I prestatori di lavoro intermittente, ripartito a tempo parziale, *ex* D.Lgs. n. 276/2003;
- I lavoratori in apprendistato, *ex* D.Lgs. n. 276/2003;
- I lavoratori con contratto di inserimento *ex* D.Lgs. n. 276/2003;
- I lavoratori in distacco da altro Ente *ex* D.Lgs. n. 276/2003;

# I subordinati

- I lavoratori di altro Ente che somministra lavoro *ex* D.Lgs. n. 276/2003;
- Gli appaltatori di attività o servizi;
- Gli agenti;
- I lavoratori autonomi;
- I rappresentanti;
- I distributori;
- I consulenti aziendali;
- I consulenti e i prestatori d'opera in *outsourcing*

# 3. INTERESSE O VANTAGGIO

- Interesse ex ante e vantaggio ex post
- Interesse e vantaggio nei reati colposi:

  volontà del legislatore di ricollegare il criterio dell'interesse o del vantaggio all'elemento costitutivo del reato presupposto rappresentato dalla **condotta** dell'autore del reato.

# Interesse e vantaggio nei reati colposi in materia di sicurezza:

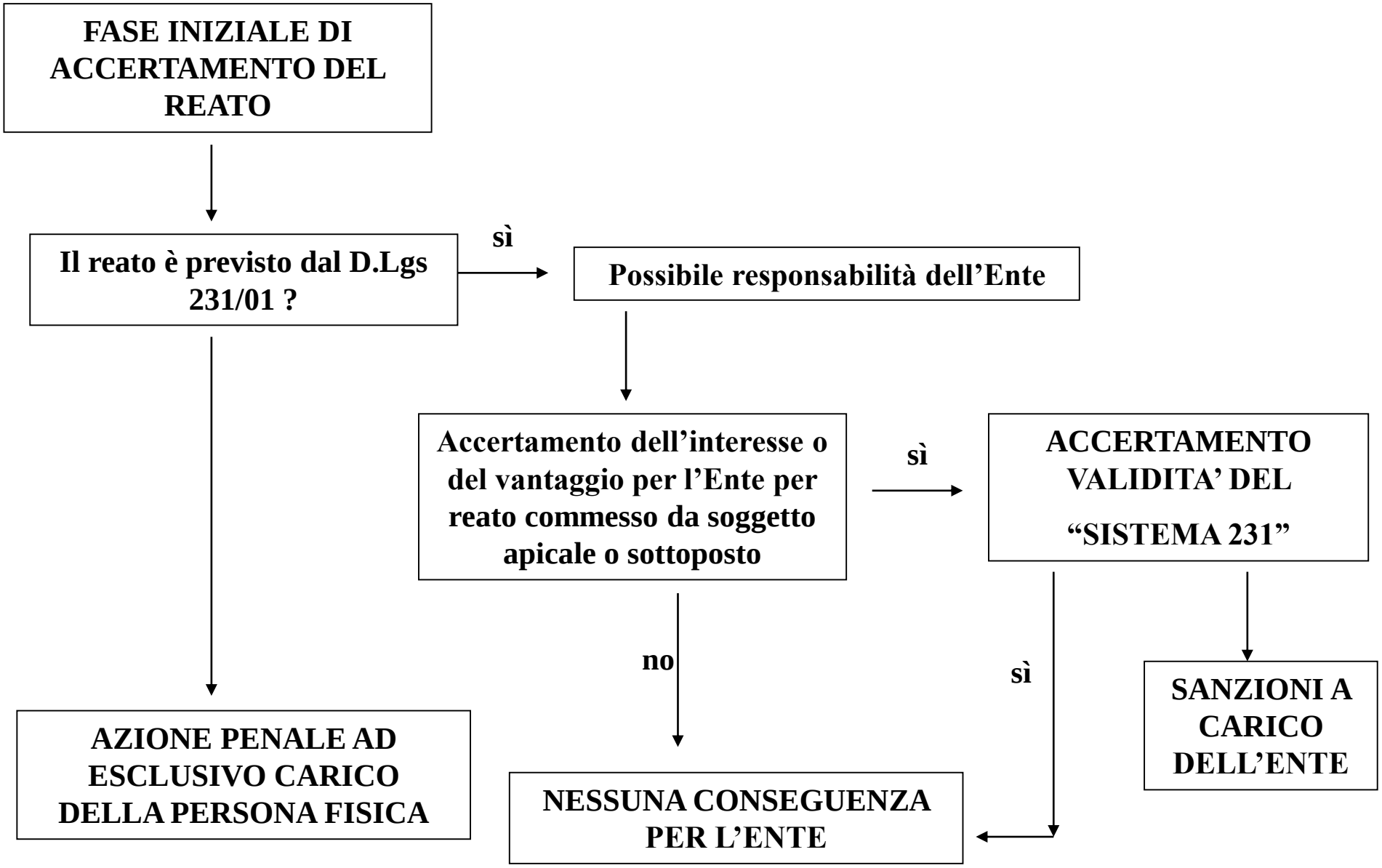
- Trib. Cagliari 4 luglio 2011:

  *"se è ben difficilmente ipotizzabile che l'evento possa rappresentare un interesse dell'ente o portare ad esso un vantaggio economico (e tanto meno non patrimoniale), è invece facilmente prevedibile che la persona giuridica possa adottare condotte tese a* ***risparmiare sui costi****, talora notevoli, connessi alla sicurezza sul lavoro".*

# Interesse e vantaggio nei reati colposi in materia di sicurezza:

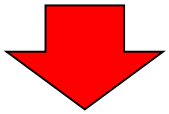
- **Corte Assise, Trib. Torino, 15 aprile 2011**

*".. Occorre, invece, che l'autore del reato abbia violato le norme di sicurezza, e, in tal guisa, cagionato la morte o la lesione, in quanto mosso, ad esempio, dalla necessità di contenere i costi produttivi, o risparmiare sulle misure di sicurezza, o accelerare i tempi o i ritmi di lavoro, o aumentare la produttività, o ancora spinto da una politica aziendale che omette investimenti in tema di sicurezza nell'ambito di uno stabilimento destinato ad essere dismesso e ciò malgrado non rinuncia a farvi lavorare gli operai".*


FASE INIZIALE DI ACCERTAMENTO DEL REATO
Il reato è previsto dal D.Lgs 231/01 ?
sì
Possibile responsabilità dell'Ente
Accertamento dell'interesse o del vantaggio per l'Ente per reato commesso da soggetto apicale o sottoposto
sì
ACCERTAMENTO VALIDITA' DEL "SISTEMA 231"
SANZIONI A CARICO DELL'ENTE
sì
no
AZIONE PENALE AD ESCLUSIVO CARICO DELLA PERSONA FISICA
NESSUNA CONSEGUENZA PER L'ENTE

# Art. 6 D.Lgs. 231/01 – Condizioni per esenzione

## Esonero dalla Responsabilità Amministrativa



### Se e soltanto se…

- L'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, **modelli di organizzazione e di gestione idonei** a prevenire reati della specie di quello verificatosi
- Il compito di **vigilare** sul funzionamento e l'osservanza del modello è stato affidato a un **organismo autonomo** dell'ente dotato di poteri di iniziativa e di controllo
- Le persone hanno commesso fraudolentemente il reato in violazione dei suddetti modelli di organizzazione e gestione
- Non vi è stata omessa o insufficiente vigilanza da parte dell'organismo al quale è stato affidato questo compito

# LE SANZIONI PREVISTE DAL D.Lgs. 231/01

**Art. 9 Sanzioni:** pecuniarie, interdittive, confisca e pubblicazione sentenza

**Art. 10 : sanzione pecuniaria non inferiore a 100 né superiore a 1.000 quote**
una quota: minimo 258€ massimo 1.549€.

**Art. 13: sanzioni interdittive:** per una durata **da 3 mesi** a **2 anni**
- interdizione dall'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un
pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- divieto di pubblicizzare beni o servizi.

# Risk Assessment

Check list di documenti da analizzare per conoscere le attività aziendali:

- Statuto della società;
- Visura camerale
- Organigramma;
- Deleghe;
- Eventuali regolamenti o procedure esistenti negli ambiti elencati;

# Chek list..

- Elenco dei soggetti che gestiscono, anche di fatto, le seguenti attività:

a) gestione flussi finanziari;
b) tenuta della contabilità e bilancio;
c) gestione e presidio sicurezza;
d) rapporti con la Pubblica Amministrazione;
e) gestione sistema informatico;
f) gestione problematiche ambientali e rifiuti;
g) gestione acquisti;
h) gestione personale;

# Chek list..

- Eventuale delibera di attuazione del T.U. n. 81/2008 indicante i ruoli e le responsabilità in tema di sicurezza sul lavoro;
- Documentazione attestante l'adempimento delle prescrizioni previste dal T.U. n. 81/2008;
- Contratto standard per appalti  e modulistica contrattuale a campione;
- Bilanci degli ultimi tre anni.

# Il Risk Assessment e le interviste

La combinazione tra documenti e interviste, tra evidenze documentali e quanto raccontato da chi organizza e gestisce quotidianamente le attività aziendali a rischio, permette di formulare l'analisi del rischio più realistica possibile.

# Il Risk Assessment e le interviste

solo un *risk assessment* profondo e veritiero può portare ad un Modello Organizzativo adeguato e idoneo a prevenire i reati in quella specifica realtà aziendale.

# LA REDAZIONE DEL MODELLO 231

## Parte Generale

(Governance, Sistema Deleghe, Codice Etico, Regolamento OdV, Sistema Disciplinare)

## Parti Speciali

(una per ciascun reato da prevenire)

# Il "Sistema 231":la nomina dell'Organismo di Vigilanza

- Con "Sistema 231" si intende il **rapporto tra MOG e lavoro dell'ODV**;
- La definizione "Sistema 231" serve per dare una **connotazione dinamica** alla necessità di presidio e prevenzione del rischio di reato che costituisce il tema di fondo del D.Lgs. n. 231/2001.
- L'ODV deve impostare un **continuo *assessment*** per analizzare la presenza e la portata del rischio reato all'interno dell'azienda; deve effettuare controlli, deve preoccuparsi di svolgere formazione, deve verificare che il MOG sia adeguato ed effettivamente attuato, e deve fare tutto ciò dandone riscontro nei verbali che certificano il suo lavoro e che costituiscono un'integrazione costante dello stesso Modello.
- Il suo lavoro è importantissimo per rendere **vivo e dinamico** un MOG che deve adattarsi ad una realtà, quella aziendale, a sua volta viva e dinamica, non inscrivibile in definizioni astratte o in un quadro di ambiti operativi statici e immutabili.

# ORGANISMO di VIGILANZA

## *Nomina e compiti*

L'Organismo è nominato **dall'organo di governo** (Consiglio di Amministrazione, Amministratore Unico, etc…) con eventuale ratifica dell'Assemblea.

L'Organo di Vigilanza deve:

- **Verificare** l'adeguatezza e l'efficacia del Modello ovverosia la sua capacità di prevedere e prevenire i comportamenti non voluti
- **Svolgere** un costante assessment delle funzioni a rischio di reato
- **Aggiornare** con il proprio lavoro e i verbali delle riunioni il Modello Organizzativo in senso dinamico
- **Effettuare** formazione in materia 231
- **Relazionarsi** agli Organi societari

# ORGANISMO di VIGILANZA

## Caratteristiche

- **Autonomia e indipendenza:**

  *Budget autonomo*

  *Collocazione in posizione di staff ai massimi vertici aziendali (Consiglio di Amministrazione o Comitato per il Controllo interno)*

- **Professionalità:**

  *Dotazione di strumenti e tecniche specialistiche adeguate alle attività di ispezione e consulenza*

  *Competenze necessarie*

- **Continuità di azione**

# Parte Speciale sulla sicurezza e TU 81/08

- ***Art. 30, c. 5***

  *"In sede di prima applicazione, i modelli di organizzazione definiti coerentemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti.*

  *Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'art. 6." (Commissione consultiva permanente per la salute e la sicurezza sul lavoro).*

# Parte Speciale sulla sicurezza e TU 81/08

- Le linee guida ed il sistema di gestione relativo al British Standard OHSAS 18001:2007, possono rappresentare il miglior aiuto possibile nel predisporre i protocolli comportamentali di una parte speciale effettivamente adeguata, ma ciò non toglie che quel sistema di per sé non garantisce rispetto all'accertamento giudiziale, anche perché privo di due elementi fondamentali del Modello Organizzativo: il sistema disciplinare e l' Organismo di Vigilanza.

# D.Lgs. 231/01 e TU 81/08

- Il Principio di effettività:

quando si affronta il tema dell'organizzazione aziendale con particolare riferimento alla sicurezza sui luoghi di lavoro, non si può prescindere dal trattare i principi di effettività e dinamicità.

# Il Principio di effettività

- **Art. 299, D.Lgs. n. 81/2008 - Esercizio di fatto di poteri direttivi**

*Le posizioni di garanzia relative ai soggetti di cui all'art. 2, c. 1, lett. b) (datore di lavoro), d) (dirigente) e e) (preposto), gravano altresì su colui il quale, pur sprovvisto di regolare investitura, eserciti in concreto i poteri giuridici riferiti a ciascuno dei soggetti ivi definiti*".

- **Art. 5 del D.Lgs. n. 231/2001** individua responsabilità nell'esercizio di fatto della gestione aziendale

# Il Principio di effettività

- **Cass. pen. n. 468/1993**

*"per l'identificazione dei responsabili in materia di prevenzione degli infortuni sul lavoro, soprattutto nelle società ad organizzazione complessa, occorre far riferimento alla ripartizione interna delle singole competenze ed alla effettività delle funzioni esercitate. Ne deriva che* ***la responsabilità non può essere accollata in maniera automatica agli amministratori o ai titolari dell'impresa, ma deve essere riferita alle persone concretamente preposte alla direzione dello specifico settore".***

# Le principali figure responsabili in materia di sicurezza

- Il Datore di Lavoro;
- Il Dirigente;
- Il Preposto;
- Il RSPP.

# Il Datore di Lavoro

- art. 2, lett. b) del T.U. n. 81/2008:

  soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa.

- Il principio di effettività in materia prevenzionistica con la conseguente distinzione tra datore di lavoro giuslavoristico e uno o più datori di lavoro in senso prevenzionale

# Il Datore di Lavoro

- **Cass. pen. n. 4106/2011**

*A questo proposito emblematica è la recente pronuncia della Suprema Corte che afferma che, nel caso in cui sussistano distinte unità produttive, il Direttore di stabilimento o di una singola unità produttiva sarà pertanto qualificabile come datore di lavoro ai fini della sicurezza* ***solo*** ***se gli saranno attribuiti poteri e disponibilità finanziarie adeguate ad effettuare gli adempimenti prescritti dalla legge e solo entro quei limiti,*** *mentre, per tutti gli altri adempimenti per i quali non dispone dei mezzi e dei poteri per realizzarli, le eventuali violazioni (e relative conseguenze) non saranno a lui ascrivibili.*

# Il Datore di lavoro

Ne deriva che, per escludere la responsabilità personale del legale rappresentante (ossia datore di lavoro in senso giuslavoristico) della società, soprattutto nelle realtà di grandi dimensioni e con più unità produttive, quest'ultimo deve aver delegato soggetti competenti che effettivamente possano, in autonomia, gestire la sicurezza nelle unità dislocate a fronte delle diverse esigenze che concretamente emergono.

# Il datore di lavoro nelle diverse forme societarie

- Nelle società di capitali:

**Cass. pen. n. 43786/2010**

*Conferma la responsabilità dei membri del consiglio di amministrazione in materia di sicurezza, salva solo l'ipotesi in cui sia avvenuto un trasferimento di poteri e responsabilità all'amministratore delegato o ad altri soggetti tramite un'idonea delega in materia.*

# Il datore di lavoro nelle diverse forme societarie

- Nelle società di persone:

  *la giurisprudenza è costante nell'identificare il datore di lavoro con il socio accomandatario o con i soci amministratori.*

- Nelle società cooperative:

  **Cass. pen. n. 31385/2010** *"nelle Società Cooperative vige il principio di identificazione del datore di lavoro nel Presidente dell'impresa cooperativa, che, in quanto rappresentante legale della stessa, assume il ruolo di datore di lavoro e dunque la posizione di garanzia allo stesso attribuita dalla legge, mentre i soci della cooperativa sono equiparati ai lavoratori subordinati"*

# Il Dirigente

- art. 2, lett. d) del T.U. n. 81/2008:

  persona che, in ragione delle competenze professionali e di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando su di essa

- In virtù del principio di effettività la figura di dirigente in senso prevenzionistico non coincide necessariamente con l'inquadramento giuslavoristico

# Secondo la giurisprudenza:

il datore di lavoro deve avere la cultura e la *forma mentis* del garante del bene costituzionalmente rilevante costituito dall'integrità del lavoratore, e non deve limitarsi ad informare i lavoratori sulle norme antinfortunistiche previste, ma deve attivarsi e controllare sino alla pedanteria, che tali norme siano assimilate dai lavoratori nella ordinaria prassi di lavoro.

# Art. 16, D.Lgs. n. 81/2008 - Delega di funzioni e sub delega

- l'intento del legislatore non è quello di deresponsabilizzare il datore di lavoro, ma al contrario di responsabilizzarlo dal punto di vista delle scelte organizzative, gestionali e di controllo della Società.
- deve rispettare i requisiti tassativamente indicati dalla norma.

# Un esempio giurisprudenziale:

- **Cass. pen. n. 27433/2008**

  Nel merito è interessante una pronuncia della Suprema Corte che riconosce validità ad una delega di funzione rilasciata ad un ingegnere esterno avente ad oggetto la sicurezza di uno stabilimento con la relativa attribuzione del potere di impegnare la società per le spese necessarie, salvo preavviso al legale rappresentante.
  Il ragionamento svolto dai giudici ancora una volta si fonda sul principio di effettività, in quanto nel concreto hanno riscontrato come la predetta delega fosse chiara nell'attribuire all'ingegnere ogni potere in tema di sicurezza, salvo solo l'incombenza di avvertire la società, stante la sua estraneità all'organigramma.

# OBBLIGO DI VIGILANZA DEL DELEGANTE

Cass. Pen. n. 10702/2012

In merito alla violazione dell'obbligo di vigilanza da parte del datore di lavoro che ha delegato altro soggetto per gli aspetti operativi inerenti la gestione della sicurezza, la Suprema Corte introduce il concetto di "**vigilanza alta**" che "di certo non può identificarsi con un'azione di vigilanza sulla concreta, minuta conformazione delle singole lavorazioni che la legge affida, appunto, al garante. Se così non fosse, l'istituto della delega si svuoterebbe di qualsiasi significato".

# La sicurezza e i contratti di appalto:

## Il Datore di lavoro committente:

- deve verificare l'idoneità tecnico-professionale delle imprese appaltatrici e dei lavoratori autonomi, in relazione ai lavori, ai servizi ed alle forniture da affidare.
- occorre quindi un controllo concreto e specifico in virtù dell'attività oggetto del contratto di appalto.

# La sicurezza e i contratti di appalto:

- deve innanzitutto verificare la professionalità e l'affidabilità degli appaltatori, senza effettuare una scelta basata sul solo fattore economico del minor prezzo, spesso sintomo di tagli all'organizzazione o alla sicurezza.

- l'obbligo del datore di lavoro committente di verificare l'idoneità dell'impresa chiamata a svolgere determinati lavori, si estende a tutte le imprese, incluse eventuali imprese subappaltatrici.

# La sicurezza e i contratti di appalto:

## Datori di lavoro appaltatori o subappaltatori:

- occorre sempre valutare il caso nella sua specificità ed evitare un generalizzato ed automatico coinvolgimento della figura del committente in relazione ad infortuni riferibili a lavori oggetto del contratto di appalto.

# La sicurezza e i contratti di appalto:

- **Cass. pen. n. 15081/2010**

  *la Cassazione che ha affermato che in presenza di un contratto di appalto, non potendo esigersi dal committente un controllo pressante, continuo e capillare sull'organizzazione e sull'andamento dei lavori dell'appaltatore, occorre un attento esame della situazione fattuale ai fini dell'individuazione delle responsabilità penali in caso di infortunio.*

# Appalti e responsabilità *ex* D.Lgs. n. 231/2001

In primo luogo i Giudici verificano la sussistenza dei presupposti richiesti dal D.Lgs. 231/01:

- commissione di uno dei reati previsti dall'art. 25 septies ex D.Lgs. 231/01;
- commissione del predetto reato da parte di uno dei soggetti qualificati dall'art. 5 del D.Lgs. n. 231/2001 (apicale o subordinato della Società);
- interesse o vantaggio dell'ente medesimo derivante dalla commissione del reato, da cui possa riconoscersi colpa gestionale o organizzativa.

# Appalti e responsabilità *ex* D.Lgs. n. 231/2001

Esempio: l'interesse e il vantaggio dell'impresa appaltatrice può consistere:

- Nel risparmio dei costi in materia di sicurezza per la mancata adozione della cautele e delle misure di prevenzione previste dalla legge
- nella necessità di accelerare i tempi di consegna al fine di evitare il pagamento di eventuali penali o per terminare in anticipo il lavoro ed iniziare così una commessa nuova.

# La Giurisprudenza ex D.Lgs. 231/01 in materia di sicurezza:

- Trib. di Trani, sez. distaccata Molfetta, 26 ottobre 2009 (Omessa elaborazione del DVR su rischi specifici ed inadeguata scelta della ditta appaltatrice o *sub* appaltatrice;
- Trib. di Novara 1° ottobre 2010 (rischio da interferenze);
- Trib. di Pinerolo 23 settembre 2010 (sicurezza dei macchinari)

# Tribunale di Trani, sez. distaccata Molfetta, 26 ottobre 2009: il fatto

- La società X aveva commissionato alla società Y il trasporto di zolfo.
- In un secondo momento la società X aveva commissionato sempre alla società Y l'attività di lavaggio dei *tank container* utilizzati per convertirli al trasporto di un'altra sostanza pericolosa, l'acido solforico.
- A sua volta la società Y aveva subappaltato alla società W la attività di bonifica dei *tank container*.
- Il giorno 3 marzo 2008 un operaio della società W si introduceva, privo della prescritta imbracatura e dell'autorespiratore, in un *tank container* per le operazioni di bonifica. Purtroppo, le esalazioni di acido solforico gli facevano perdere la vita. Due colleghi cercavano di portargli soccorso, ma anche loro perdevano la vita. Stessa tragica sorte capitava al trasportatore del *tank container*, che a sua volta cercava di prestare i soccorsi. Infine moriva il titolare della ditta W anche lui accorso per aiutare i suoi collaboratori. Un ultimo operaio si affacciava al boccaporto del *tank container* e a causa delle esalazioni riportava lesioni gravi.

# Tribunale di Trani, sez. distaccata Molfetta, 26 ottobre 2009:

La sentenza afferma alcuni fondamentali principi:

- *"il sistema introdotto dal D.Lgs. n. 231/2001* ***impone alle imprese di adottare un modello organizzativo diverso e ulteriore rispetto a quello previsto dalla normativa antinfortunistica,*** *onde evitare in tal modo la responsabilità amministrativa*";

# Tribunale di Trani, sez. distaccata Molfetta, 26 ottobre 2009:

- *l'impostazione del Modello Organizzativo non deve esaurirsi nella prevenzione degli infortuni dei propri dipendenti o di soggetti presenti nel proprio ambiente e quindi solo nell'ambito della propria struttura organizzativa ed aziendale, ma* ***deve estendersi anche ai dipendenti di altre società che, direttamente o indirettamente, entrano in contatto con la società stessa, svolgendo servizi nell'interesse della medesima.***

# Tribunale di Trani, sez. distaccata Molfetta, 26 ottobre 2009:

La sentenza appena descritta fornisce indicazioni fondamentali per poter predisporre un idoneo ed efficace Modello Organizzativo e Gestionale in grado di prevenire e minimizzare concretamente il rischio di reato in materia di sicurezza.

# Trib. Novara 1 ottobre 2010 (Il rischio da interferenze): il fatto

- la società X (s.r.l.) effettua la manutenzione ordinaria degli immobili e delle infrastrutture del C.I.M. di Novara e si occupa del carico e dello scarico dei *container* dei treni;
- la società Y(S.p.A.), su incarico della società X, effettua le manovre di introduzione o estrazione dei treni dal C.I.M. di Novara;
- la società W (società cooperativa esercente attività di servizi alle aziende pubbliche e private), sempre per conto della società X, effettua la spunta dei treni e il controllo del loro carico.
- In data 26 ottobre 2007 alle ore 6.15 circa un dipendente della cooperativa W usciva dagli uffici per andare a controllare un treno su un binario del C.I.M. Effettuata, come previsto, la spunta al treno, entrava nell'ufficio di un collega, il RSPP della società X. Successivamente alle ore 7,10 circa decideva di recarsi presso gli uffici della cooperativa W e mentre attraversava i binari, in corrispondenza del passaggio pedonale previsto dalla viabilità interna, veniva investito da un locomotore e rimaneva ucciso.

# Trib. Novara 1 ottobre 2010 (Il rischio da interferenze)

Nel caso di specie è stato accertato il nesso causale tra l'evento-infortunio che ha causato la morte di un dipendente della cooperativa W e **la colpa organizzativa e gestionale** in capo alle Società X s.r.l. e alla stessa cooperativa W, soprattutto sotto il profilo della violazione dell'obbligo, sancito dall'art. 26, T.U. n. 81/2008, di cooperare e coordinare con tutti i datori di lavoro coinvolti nell'esercizio delle diverse attività oggetto dell'appalto di servizi, nonostante le evidenze e la conoscenza dei rischi derivanti dalla circolazione dei treni e del personale a piedi del terminal.

# Trib. Novara 1 ottobre 2010 (Il rischio da interferenze)

- *interesse o vantaggio:*

*"non adottando le indispensabili iniziative volte a prevenire il rischio di investimento ferroviario,*

*riducevano ed evitavano i costi degli interventi strumentali necessari (ad esempio installazione di un articolato sistema di segnali acustici e visivi, manutenzione dei presidi esistenti),*

*velocizzavano i tempi e i ritmi del ciclo produttivo, evitavano i disagi organizzativi e l'utilizzo del tempo per lo svolgimento dell'attività di coordinamento e cooperazione,*

*riducevano i costi per la formazione e l'informazione del personale".*

# Uso del DPI e sicurezza dei macchinari

- Art. 71, D.Lgs. n. 81/2008 - Obblighi del datore di lavoro

- **Cass. pen. n. 7294/2010**

*"non vi è un automatismo tra la presenza di una dichiarazione di conformità CE del macchinario e l'esenzione di responsabilità del datore di lavoro, allorquando il vizio da cui deriva l'infortunio è tutt'altro che occulto o invisibile".*

# Uso del DPI e sicurezza dei macchinari

- Tribunale di Pinerolo (sentenza del 23 settembre 2010): il fatto.

Si tratta di un caso che ha visto l'infortunio di un dipendente che, nell'utilizzare una macchina deputata allo schiacciamento di polpe da barbabietole esauste per la riduzione in farina, al fine di rimuovere dai rulli pietre che inceppavano il funzionamento, senza spegnere la macchina, rimuoveva lo sportello a protezione dei cilindri laminatoi e vi infilava la mano, venendo poi afferrato con conseguente trascinamento e schiacciamento dell'arto fra i cilindri.

# Tribunale di Pinerolo (sentenza del 23 settembre 2010)

È stato accertato un omesso controllo e un'indifferenza rispetto allo stato della sicurezza del macchinario ed alle problematiche che erano state segnalate proprio dal dipendente infortunato, tali da integrare gli estremi di "una inaccettabile negligenza".

# Tribunale di Pinerolo (sentenza del 23 settembre 2010)

- *si tratta di un classico reato colposo commesso da un datore di lavoro che è apparso indifferente, o comunque non sufficientemente attento, alla tutela delle condizioni di lavoro dei propri dipendenti;*
- *la società non si era dotata di un Modello Organizzativo, nemmeno dopo l'infortunio;*
- *non ricorrono nel caso di specie le condizioni di esonero da responsabilità previste dall'art. 6 ex D.Lgs. n. 231/2001.*

# Il Preposto

- art. 2, lett. e) del T.U. n. 81/2008 ne fornisce la definizione:

  persona che, in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende alla attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa

- secondo il principio di effettività "*la qualifica e le responsabilità del preposto non competono soltanto ai soggetti forniti di titoli professionali o di formali investiture, ma a chiunque si trovi in una posizione di supremazia sia pure embrionale, tale cioè da porlo in condizione di dirigere l'attività lavorativa di altri operai soggetti ai suoi ordini*".

# Il RSPP

- Persona in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi.
- Art. 33, D.Lgs. n. 81/2008 - Compiti del servizio di prevenzione e protezione
- Oggi non è escluso che accanto ad una responsabilità del datore di lavoro che rimane titolare della "posizione di garanzia", si possa configurare anche una responsabilità concorrente del RSPP.

# Il RSPP

- **Cass. pen., 19 luglio 2011, n. 28779**

  *"anche il RSPP, infatti, che pure è privo dei poteri decisionali e di spesa (e quindi non può direttamente intervenire per rimuovere le situazioni di rischio), può essere ritenuto (cor)responsabile del verificarsi di un infortunio, ogni qualvolta questo sia oggettivamente riconducibile ad una situazione pericolosa che egli avrebbe avuto l'obbligo di conoscere e segnalare, dovendosi presumere che alla segnalazione avrebbe fatto seguito l'adozione, da parte del datore di lavoro, delle necessarie iniziative idonee a neutralizzare detta situazione".*

# Il RSPP

- Cass. pen. n. 2814 del 27 gennaio 2011:

  *"Non è pertanto dubitabile, la posizione di garanzia in cui si trovava il (...), nella qualità di responsabile della sicurezza, in ragione dei propri compiti all'interno dell'azienda,* ***che gli imponevano di attivarsi positivamente per organizzare le attività lavorative in modo sicuro,*** *provvedendo alla individuazione e valutazione dei fattori di rischio, all'obbligo di formazione e di vigilanza dei lavoratori finalizzato proprio ad evitare incidenti come quello verificatosi".*

# Altre figure responsabili in materia di sicurezza

- Il responsabile ufficio acquisti;
- Il responsabile ufficio personale;
- Il medico competente;
- Il lavoratore.

# Il Caso ThyssenKrupp: sentenza Corte di Assise Trib. Torino 15 aprile 2011

Si presti attenzione alle seguenti circostanze:

- una grave situazione aziendale in tema di sicurezza, accertata dai vertici aziendali col supporto di tecnici qualificati, e che ha visto gravi precedenti nel settore specifico che ha dato origine all'infortunio;
- un amministratore delegato - datore di lavoro con grande conoscenza tecnica in materia di sicurezza e grande consapevolezza dei problemi esistenti in azienda;
- la decisione di continuare a produrre, ma di non investire nulla per la sicurezza, perché da lì a un anno circa la produzione sarà trasferita in altra sede, nonostante l'alto grado di consapevolezza del rischio e dei precedenti incidenti;
- la decisione di non effettuare gli interventi in materia di sicurezza, perché li si subordina agli obiettivi economici aziendali;
- l'impossibilità oggettiva di sperare ragionevolmente che non capiti alcun incidente nelle condizioni attuali.

# Il Caso ThyssenKrupp: sentenza Corte di Assise Trib. Torino 15 aprile 2011

- Interesse e vantaggio:

  *"le gravissime violazioni della normativa antinfortunistica ed antincendio (v. i vari capitoli precedenti), le colpevoli omissioni, sono caratterizzate da un contenuto economico rispetto al quale l'azienda non solo aveva interesse, ma se ne è anche sicuramente avvantaggiata, sotto il profilo del considerevole risparmio economico che ha tratto omettendo qualsiasi intervento nello stabilimento di Torino; oltre che dell'utile contemporaneamente ritratto dalla continuità della produzione".*

# Il Caso ThyssenKrupp: sentenza Corte di Assise Trib. Torino 15 aprile 2011

- L'assenza di un Modello Organizzativo:

  *"La mancata adozione di tali modelli, in presenza dei presupposti oggettivi e soggettivi sopra indicati (reato commesso nell'interesse o vantaggio della società e posizione apicale dell'autore del reato) è sufficiente a costituire quella 'rimproverabilità' di cui alla relazione ministeriale al decreto legislativo e ad integrare la fattispecie sanzionatoria, costituita dall'omissione delle previste doverose cautele organizzative e gestionali idonee a prevenire talune tipologie criminose".*

# Best Practices

- Comunicazione e formazione
- Coinvolgimento diretto
- Aspetti contrattuali legati al tema degli appalti
- OdV e consulenti esterni

«*Whistleblower*» è chi conosce di un illecito o di un'irregolarità sul luogo di lavoro, durante lo svolgimento delle proprie mansioni, e decide di segnalarlo a una persona o a un'autorità che possa agire efficacemente al riguardo.

Pur rischiando atti di ritorsione a causa della segnalazione, egli svolge un ruolo di interesse pubblico, dando conoscenza di problemi o pericoli all'ente di appartenenza o alla comunità.

Il «*whistleblowing*», quindi, è l'attività di regolamentazione delle procedure volte a incentivare e proteggere tali segnalazioni.

Dalla definizione dell'istituto discende che per attivare un corretto

**sistema di segnalazione**

gli aspetti centrali sono

- la disciplina esaustiva del **flusso informativo**
- la **riservatezza** circa l'identità del soggetto segnalante, del soggetto segnalato e del contenuto della segnalazione
- la **tutela** del soggetto segnalante da atti ritorsivi e/o discriminatori, anche solo potenziali

## 1. L'atto di comunicazione

Può essere **formale** o **informale** ed è realizzato dal WB

- in assoluta autonomia oppure
- a seguito di un obbligo di *reporting* legato al proprio ruolo nell'organizzazione

## 2. Il profilo del *whistleblower*

Secondo *Transparency International*

«*A whistleblower is any public or private sector employee or worker who discloses information about these types of wrongdoing and who is at risk of retribution.*

*This includes individuals who are outside the traditional employee-employer relationship, such as consultants, contractors, trainees or interns, volunteers, student workers, temporary workers, and former employees*»

Quindi un WB potrebbe essere un dipendente, un consulente, un fornitore o persino un cliente

3. **Lo strumento di segnalazione** ossia il canale informativo

4. **L'oggetto della comunicazione** è il «*wrongdoing*», che può essere

- un comportamento scorretto già in essere o
- un comportamento censurabile che secondo la percezione del WB potrebbe essere posto in essere in futuro

## Meritano attenzione

- la **Convenzione Civile sulla Corruzione** firmata a Strasburgo nel 1999, che all'art. 9 prevede una protezione adeguata per i dipendenti i quali, in buona fede e sulla base di ragionevoli sospetti, denuncino fatti di corruzione alle persone o autorità responsabili

- la **Convenzione delle Nazioni Unite** del 2003, che all'art. 33 richiede a ciascuno Stato Parte di prevedere meccanismi di protezione per le persone che riferiscono su fatti di corruzione

In tale contesto, la giurisprudenza della Corte Europea dei Diritti dell'Uomo ha un ruolo chiave nello stabilire ed espandere gli standard di tutela dei WB.

Per i giudici di Strasburgo il *whistleblowing* è strettamente connesso al diritto alla **libertà di espressione** garantito dall'art. 10 della Conv. EDU, che include la libertà «di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera»,

prevedendo **restrizioni** in alcuni casi eccezionali.

Nei casi di WB, tali restrizioni possono riguardare interessi individuali quali il diritto alla privacy e la dignità personale, ovvero interessi superindividuali come la sicurezza nazionale

# Alcune pronunce della Corte in materia di WB

Con la sentenza **Guja *vs* Moldova** (2008), la Corte ha riconosciuto che il diritto alla libertà di espressione (art. 10 Conv. EDU) è stato violato quando un pubblico ufficiale presso la Procura generale moldava è stato licenziato dopo aver reso pubblici dei documenti interni comprovanti un tentativo di corruzione dell'autorità giudiziaria.

Anche nel caso **Bucur *vs* Romania** (2013) la Corte ha sentenziato che l'arresto di un *whistleblower* sulla base della rivelazione di informazioni riservate violava il diritto alla libertà di espressione (art. 10 Conv. EDU), nonostante il caso coinvolgesse la sicurezza nazionale e i servizi segreti.

Con la **l. n. 190/2012 ("Legge anticorruzione")** è stata introdotta nell'ordinamento italiano la prima forma di tutela espressa della figura del WB, seppur circoscritta al settore del **pubblico impiego**.

All'**art. 54 *bis*** d.lgs. n. 165/2001 ("TU Pubblico Impiego") si è delineata la **tutela del dipendente pubblico che segnala illeciti**, prevedendo

- **Tutela del posto di lavoro**: il pubblico dipendente che denuncia o riferisce condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro non può essere sanzionato, licenziato o sottoposto a una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia
- **Tutela dell'identità del segnalante**: viene stabilito che l'identità del segnalante non può essere rivelata nell'ambito del procedimento disciplinare senza il suo consenso, con due rilevanti eccezioni
  - la contestazione dell'addebito disciplinare contro la persona oggetto della segnalazione sia fondata esclusivamente sul contenuto della segnalazione stessa
  - la conoscenza dell'identità del segnalante sia assolutamente indispensabile per ragioni di difesa del segnalato

## La l. n. 190/2012 ha inoltre disposto

- l'esclusione della protezione del segnalante nei casi in cui il WB commetta un reato di calunnia, di diffamazione o abbia causato un danno ingiusto (*ex* art. 2043 c.c.)
- l'operatività della tutela solamente laddove la segnalazione sia indirizzata all'Autorità giudiziaria, alla Corte dei Conti, all'ANAC o al superiore gerarchico
- l'esclusione della segnalazione dal diritto d'accesso previsto dalla legge sul procedimento amministrativo (artt. 22 ss. l. n. 241/1990)

Come emerge dall'art. 54 *bis* d.lgs. n. 165/2001

i rischi penali cui va incontro il segnalante

**in mala fede**

sono quelli di commettere

il reato di calunnia

il reato di diffamazione

In tale contesto assumono centrale rilevanza le

Linee Guida ANAC
[Determinazione n. 6 del 28.04.15]

**OBIETTIVO**

offrire alle amministrazioni pubbliche italiane
una disciplina applicativa
rispetto alle disposizioni della l. n. 190/2012
attraverso un modello procedurale
per il trattamento delle segnalazioni

Numerose sono state le critiche all'**art. 54 *bis***, ritenuto non in grado di incentivare le denunce da parte dei dipendenti pubblici e, semmai, in grado di disincentivarle a causa della sua **ambigua formulazione**.

Tra le altre cose, la norma è stata censurata laddove

- individua solo quattro soggetti idonei a ricevere la denuncia (Autorità giudiziaria, Corte dei Conti, ANAC e superiore gerarchico), senza specificare se vi siano casi dove il WB debba preferire un determinato soggetto (come invece avviene nel Regno Unito)
- non richiede l'istituzione di unità specifiche all'interno degli enti per la gestione delle segnalazioni

- non tutela i dipendenti **privati**, collaboratori, appaltatori, stagisti

- tutela solo le segnalazioni in cui il dipendente sia venuto a conoscenza delle condotte illecite **in ragione del** rapporto di lavoro

- il **diritto di accesso** (del segnalato) all'identità del segnalante sussiste in casi che non sono nella disponibilità del WB («qualora la contestazione sia fondata in tutto o in parte sulla segnalazione, l'identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa dell'incolpato»)

- non prevede una forma specifica di responsabilità penale nei confronti del datore di lavoro che ostacoli intenzionalmente l'invio delle segnalazioni alle autorità competenti

- non incentiva le segnalazioni con **ricompense**

- non richiede attività di **sensibilizzazione** agli enti preposti, come il Ministero della Pubblica Amministrazione e la Semplificazione e il Ministero dell'Istruzione, dell'Università e della Ricerca

- All'ANAC nei primi 5 mesi del 2017 ne sono arrivate 263 rispetto alle 252 dell'intero 2016
- Arrivano per il 75% dalle prime linee della P.A. (impiegati, insegnanti e personale sanitario), mentre sono molte meno quelle dagli alti livelli della P.A. (dirigenti, responsabili della prevenzione della corruzione, vertici militari)
- Le condotte illecite segnalate riguardano soprattutto gli appalti pubblici, l'attribuzione di incarichi pubblici e i concorsi pubblici

# Legge 30 novembre 2017 n. 179

«Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro **pubblico** o **privato**»

**In vigore dal 29 dicembre 2017**


Si compone di **3 articoli**
e mira, soprattutto, alla tutela dei lavoratori segnalanti

**Art. 1**: la **P.A.** modifica l'**art. 54 *bis* del TU Pubblico impiego**

**Art. 2**: il **settore privato** modifica l'**art. 6 del d.lgs. n. 231/2001**

**Art. 3**: **scriminante rivelazione segreto**

La segnalazione nell'interesse all'integrità delle amministrazioni (**pubbliche o private**) e alla prevenzione e repressione delle malversazioni costituisce

**giusta causa**

- di rivelazione di notizie coperte dal segreto d'ufficio, professionale, scientifico e industriale (artt. 326, 622, 623 c.p.)
- di rivelazione di notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa (art. 2105 c.c.)

La norma NON si applica però ai rapporti di consulenza o di assistenza, o nel caso in cui il segreto sia rivelato con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, al di fuori del canale di comunicazione predisposto a tal fine

## 1. WB più garantito

Il **dipendente pubblico** che segnala ai responsabili anticorruzione, all'ANAC o ai magistrati ordinari e contabili illeciti che abbia conosciuto **in ragione del rapporto di lavoro** non può essere sanzionato, demansionato, licenziato, trasferito o sottoposto ad altra misura organizzativa avente effetti negativi (diretti o indiretti) sulle condizioni di lavoro determinata dalla segnalazione.

**rt. 1: la P.A.**

modifiche
ll'**art. 54 *bis***
l **TU pubblico impiego**

Dal punto di vista soggettivo, l'**ambito di applicazione è allargato** a ulteriori categorie di dipendenti pubblici e ai lavoratori, collaboratori e consulenti degli enti pubblici economici, a quelli degli enti di diritto privato sottoposti a controllo pubblico, nonché ai lavoratori e collaboratori a qualsiasi titolo, di imprese fornitrici di beni o servizi che realizzano opere in favore della P.A.

Dal punto di vista oggettivo, la tutela riguarda le segnalazioni o denunce effettuate **nell'interesse dell'integrità della P.A.**

## 2. Segretezza identità

L'identità del WB, nell'ambito del

- **processo penale:** è coperta dal segreto nei limiti del c.p.p.
- **procedimento** davanti **Corte dei Conti:** non può essere rivelata fino alla chiusura della fase istruttoria
- **procedimento disciplinare:** non può essere rivelata se la contestazione dell'addebito è fondata su accertamenti ulteriori rispetto alla segnalazione

L'ANAC, sentito il Garante Privacy, adotta apposite **linee guida** relative alle procedure per la presentazione e la gestione delle segnalazioni.
Le linee guida prevedono l'utilizzo di modalità informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza del segnalante, del contenuto della segnalazione e della relativa documentazione

## 3. Sanzioni

L'ANAC, a cui l'interessato o i sindacati comunicano eventuali atti discriminatori, applica al responsabile una **sanzione amministrativa pecuniaria** da € 5.000 a € 30.000.
La mancata verifica della segnalazione e l'assenza o l'adozione di procedure discordanti dalle linee guida comportano una sanzione amministrativa pecuniaria da € 10.000 a € 50.000.

## 4. Atti discriminatori nulli

Sono previsti il **reintegro** nel posto di lavoro in caso di licenziamento e la **nullità** di ogni **atto** discriminatorio o ritorsivo. L'**onere della prova** è **invertito**: spetta all'ente dimostrare l'estraneità della misura adottata rispetto alla segnalazione.

# 5. Clausola «anti-calunnia»

Ogni tutela per il WB non è più garantita nei casi in cui sia accertata

- la **responsabilità penale** del segnalante, anche con sentenza di primo grado, per i reati di calunnia o diffamazione o, comunque, per reati commessi con la denuncia, ovvero
- la sua **responsabilità civile**, per lo stesso titolo, nei casi di dolo o colpa grave.

# Tutela dell'identità del segnalante

- Tutela rafforzata: qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità.

# ...con inversione dell'onere della prova...

- È a carico dell'amministrazione pubblica dimostrare che le misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione. Gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente sono nulli.


Art. 2
Settore privato
modifiche all'art. 6 del d.lgs. n. 231/2001
All'art. 6 d.lgs. n. 231/2001 dopo il comma 2 sono inseriti 3 nuovi commi
2 bis
Prevede significative modifiche ai modelli di organizzazione e gestione di cui al co.1 lett. a)
2 ter
Prevede la possibilità di denunciare l'adozione di misure discriminatorie all'Ispettorato Nazionale del Lavoro.
2 quater
Sancisce la nullità del licenziamento e di ogni altra misura ritorsiva o discriminatoria adottata nei confronti del WB. Disciplina l'onere della prova

**Art. 2**
**Settore privato**
modifiche all'**art. 6**
del **d.lgs. n. 231/2001**

## Nuovo comma 2 *bis*

I modelli di organizzazione e gestione prevedono

***a)*** uno o più **canali** che consentano ai soggetti di cui all'art. 5, co. 1, *lett. a)* e *b)** di presentare

**a tutela dell'integrità dell'ente**
**segnalazioni circostanziate**

- di condotte illecite rilevanti ai sensi del d.lgs. n. 231/2001 e fondate su elementi di fatto precisi e concordanti o
- di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte

Tali canali garantiscono la **riservatezza** dell'identità del segnalante nelle attività di gestione della segnalazione

(*) ossia: *«a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)».*

# Nuovo comma 2 *bis*

I modelli di organizzazione e gestione prevedono

***b)*** almeno un **canale alternativo** di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante

***c)*** il **divieto** di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione

***d)*** nel **sistema disciplinare** adottato ai sensi del co. 2 lett. *e)**, **sanzioni** nei confronti

- di chi viola le misure di tutela del segnalante
- di chi effettua con dolo o colpa grave segnalazioni che si rivelino infondate

# Nuovo comma 2 *ter*

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al co. 2 *bis* può essere **denunciata** all'Ispettorato Nazionale del Lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

# Nuovo comma 2 *quater*

Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è **nullo**.
Sono altresì nulli il mutamento di mansioni ai sensi dell'art. 2103 c.c., nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante.

È **onere del datore di lavoro**, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, **dimostrare** che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

L'aspetto essenziale della legge
è che essa è rivolta solo agli
**enti che hanno adottato un Modello**
di organizzazione e gestione ai sensi del d.lgs. n. 231/01

La portata innovativa della riforma si esaurisce, infatti,
nell'introdurre **nuovi requisiti di idoneità**
dei modelli 231, che (come noto) sono facoltativi

Il WB viene ricompreso nell'art. 6 sui flussi informativi che devono pervenire all'ODV.
Il nuovo co. 2 *bis*
non menziona però l'ODV come destinatario

→ Destinatario della segnalazione può essere un soggetto/comitato distinto, in tutto o in parte, dall'ODV?

La tutela prevista per i soggetti (pubblici o privati) danneggiati da denunce infondate è limitata

→ **Nel pubblico**: rispetto al testo originario del d.d.l. è stata soppressa la possibilità di licenziamento per giusta causa in caso di falsa segnalazione

→ **Nel privato**: WB responsabile solo nel caso di dolo o colpa grave

La nuova legge richiede che i canali di segnalazione garantiscano la «**riservatezza**» dell'identità del denunciante.

Il profilo della «riservatezza» è diverso da quello dell'«**anonimato**».
Come chiarito dalle Linee Guida ANAC (determinazione n.6/2015) il primo presuppone la rivelazione della propria identità da parte del denunciante che, infatti, «può godere di una tutela adeguata solo se si rende riconoscibile».

Ciò non esclude che i Modelli Organizzativi possano contemplare anche **canali per le segnalazioni anonime**.

L'ODV potrebbe essere individuato come «destinatario autonomo e indipendente» delle denunce.

Tale soluzione sembra realizzare con efficacia le finalità della nuova disciplina, di salvaguardare l'integrità dell'ente e tutelare il segnalante.

Se l'ODV non è individuato come destinatario esclusivo, sembra comunque opportuno prevedere il suo coinvolgimento in via concorrente ovvero successiva, per evitare il rischio che il flusso di informazioni generato dal nuovo meccanismo di WB sfugga del tutto dal controllo dell'ODV.

Tale meccanismo, infatti, «è una parte del più ampio Modello Organizzativo di cui l'ODV è tenuto a verificare il funzionamento».

# *M4.5 Integrazione Modello Organizzativo 231 e Modello Privacy*

***Avv. Ida Tascone***

# 1. Il modello organizzativo 231: da vincolo a opportunità

## 1.1 L'adozione di un mo231 quale adempimento delle previsioni di legge: effetto ed efficacia esimente per le rilevanti sanzioni previste dalla relativa disciplina.

## Perché adottare un MO231 quale vantaggio competitivo in termini di business per management/proprietà: aspetti reputazionali e creazione del valore.

***

La scelta di adottare un Modello Organizzativo, non è stata imposta da fattori esogeni, bensì da una volontà precisa e ferma del Management di dotarsi di un Sistema complesso e articolato che permettesse non solo di garantire una adeguata supervisione dei processi critici dell'Azienda, bensì anche per presentarsi sul mercato con una identità forte, di Impresa attenta e oculata alla propria gestione, che si potesse distinguere dalla pluralità dei propri competitor e non, come una Società solida, che cura in ogni dettaglio il proprio Business.

Nel considerare l'opportunità di dotarsi di un modello organizzativo idoneo a prevenire i reati occorre tener conto di tutti i possibili vantaggi. Gli obiettivi delle aziende che guardano al futuro non sono più solo legati esclusivamente alla mera sfera economica, ma tendono ad inglobare scenari più ampi, legando l'organizzazione alla sostenibilità dell'ambiente ad essa circostante.

Non è una scelta limitata alle grandi aziende ma rappresenta un vantaggio competitivo che impatterà sulla sopravvivenza delle piccole e medie imprese.

I vantaggi sono riscontrabili sotto diversi profili: strategici e reputazionali, economici, compliance. In particolare scegliere di adottare un modello organizzativo:

- costituisce un elemento sempre più diffuso di valutazione nella scelta e selezione dei partner commerciali
- consente una gestione del business trasparente e corretta
- favorisce la chiarezza organizzativa ed il corretto bilanciamento tra poteri e responsabilità, grazie al riesame di deleghe e procure a rappresentare l'azienda verso i fornitori e ad operare sui conti bancari

- aumenta la diffusione della cultura della gestione dei rischi e dei controlli sulle operazioni di business
- tutela il vertice apicale
- agevola l'analisi delle inefficienze e la risoluzione delle problematiche di gestione delle organizzazioni, evidenziando le opportunità di miglioramento di tutti i principali processi aziendali
- migliora il processo di acquisti /approvvigionamenti
- assicura il rispetto delle normative correlate, quali la salute e sicurezza nei luoghi di lavoro, ambiente, area finance, etc.
- riduce al minimo il verificarsi di infortuni sul lavoro, malattie professionali, incidenti ambientali, affidamento incauto di lavori, servizi, forniture, appalti e subappalti a fornitori non in possesso dei requisiti tecnico professionali

- riduce il rischio di sanzioni (pecuniarie o interdittive) con potenziali gravissimi danni patrimoniali e d'immagine alle società
- evita il formarsi di pratiche corruttive all'interno dell'organizzazione
- aumenta l'engagement (motivazione) dei dipendenti e la creazione di un clima di fiducia e di condivisione, incrementando il livello di innovazione dell'impresa e la sua capacità di adattamento ai cambiamenti
- aumenta lo sviluppo professionale dei dipendenti grazie alla formazione continua e mirata

La prima affermazione che viene da fare in merito all'adozione di un Modello Organizzativo secondo il D. Lgs. 231/2001 è che non è un processo semplice, bensì complesso e complicato allo stesso momento. Questo perché tutto dipende dalle dimensioni, dal settore e dalla struttura organizzativa stessa dell'azienda.

Il vantaggio principale dell'adozione di un Modello Organizzativo è anzitutto l'opportunità di effettuare una profonda analisi dell'azienda, in quanto fase necessaria nel momento della sua impostazione, facendo "emergere" agli occhi del Management non solo i processi chiave dell'Azienda, bensì anche le procedure e i processi che solitamente vengono visti come "minori" ma che, in ottica strategica, possono rilevarsi di fondamentale importanza, se sottostimati o se addirittura ignorati, in quanto permettono di avere una visione olistica dell'Azienda e permettono di capire i vari livelli di Responsabilità a cui sono affidati e se vengono correttamente rispettati o applicati o se vi sono criticità che, alla lunga, potrebbero anche comportare enormi problematiche da gestire in futuro.

Il decreto legislativo 231/2001, come noto, prevede l'adozione di Modelli di organizzazione gestione e controllo con valore di prevenzione alla commissione di reati previsti dal Decreto stesso, al fine di poter costituire una idonea "misura di difesa", nel caso di imputazione dell'Ente per la sua "responsabilità amministrativa".

Le caratteristiche di tali modelli di esonero sono definite dagli art. 6 e 7 del decreto.

In sintesi essi devono caratterizzarsi, per una positiva valutazione dei medesimi, per i seguenti criteri:

- devono prevedere le attività nel cui ambito possano essere commessi i reati;
- devono prevedere specifici "protocolli" (ovvero procedure) diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire,
- devono individuare le modalità di gestione delle risorse destinate alle misure impeditive della commissione dei reati;

- devono stabilire obblighi di formazione nei confronti dell'organismo nominato per la vigilanza del modello;
- devono introdurre un sistema disciplinare per il mancato rispetto delle misure indicate nel modello.

Un Modello (quando esso si articola in diversi documenti si parla complessivamente di "Modelli" come riferimento a tutta la documentazione da esso richiamata), qualora risultasse carente o mancante, determinerebbe una colpa di organizzazione fondata sul rimprovero di non aver adottato quelle cautele organizzative e gestionali necessarie a prevenire la commissione dei reati fondanti la responsabilità del soggetto collettivo.

Non trovando altri riferimenti alle caratteristiche dei "Modelli 231/2001" nel testo del Decreto, l'attenzione va quindi posta alle sentenze dei Giudici e alle Linee guida della Associazioni di Categoria.

La giurisprudenza, anche di Cassazione, spesso si è concentrata proprio sul giudizio di idoneità dei Modelli, precisando, in definitiva, che tali accorgimenti devono essere *consacrati in un documento che individua i rischi e delinea le misure atte a contrastarli.*

## La mappatura del rischio

Sulla scorta dei predetti richiami (testo del decreto legislativo, codici di comportamento associativi, indicazioni giurisprudenziali,) i Modelli 231/2001 sono stati nel tempo prodotti, dalle organizzazioni che hanno ritenuto opportuno dotarsi di un Organismo di Vigilanza, a seguito di "mappature" dei rischi nei processi aziendali. Contestualmente sono stati individuati i cosiddetti "presidi" posti a mitigazione dei rischi-reato richiamati dal Decreto, sia di tipo organizzativo, che di tipo procedurale o informatico.

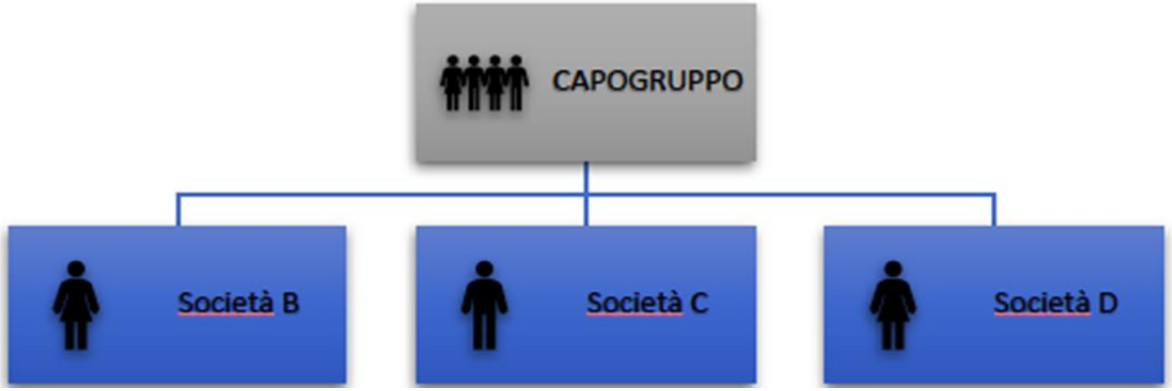
I primi esempi di mappature del rischio e del controllo "231/2001" sovente rimandavano ad alti principi aziendali o all'eticità dell'impresa; successivamente, anche a seguito della produzione giurisprudenziale che ne ha sancito l'inadeguatezza e all'incremento delle fattispecie di rischio previste dal legislatore, i riferimenti alle modalità di prevenzione sono stati sempre più puntuali e diretti alle procedure adottate dall'Ente.

# Esercizio del potere disciplinare, rispetto della normativa sulla privacy e adeguamento del modello 231/2001 e regolamenti aziendali

- **Aggiornamento del Modello Organizzativo 231/2001 nella parte relativa alle sanzioni disciplinari;**
- **Aggiornamento Regolamenti aziendali;**
- **Aggiornamento Codici disciplinari.**

## Caratteristiche dell'Organismo di Vigilanza


## Composizione OdV nel Gruppo



I codici di condotta sono regole di condotta o pratiche uniformi elaborate da vari organismi internazionali o anche da singoli Stati, particolarmente diffuse nei rapporti economici internazionali. In genere contengono disposizioni non vincolanti anche se l'autorevolezza dell'organismo da cui promanano fanno si che siano di larga e diffusa applicazione.

Il regolamento europeo n. 679/2016 contiene un grosso incoraggiamento all'utilizzo dei codici di condotta, ma ovviamente in un'ottica comunitaria.
In effetti il GDPR all'art. 40 sancisce che gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono, quindi, elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione delle disposizioni del Regolamento.

Si pensi:
a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;
g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli articoli 24 e 25 del GDPR e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;
i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;
k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79 del GDPR.

Le associazioni e gli altri organismi previsti dal Regolamento che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice all'autorità di controllo (cioé al nostro Garante). L'autorità di controllo esprime un parere sulla conformità al Regolamento del progetto di codice o del codice modificato o prorogato e lo approva, se ritiene che offra garanzie sufficientemente adeguate. In questo caso l'autorità di controllo registra e pubblica il codice.

Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvare il progetto, la modifica o la proroga, l'autorità di controllo che è competente ai sensi dell'articolo 55 del regolamento lo sottopone, tramite la procedura di coerenza, al comitato, il quale formula un parere sulla conformità al regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 dell'art. 40 del GDPR, sulla previsione di adeguate garanzie.

Qualora il parere confermi che il progetto di codice di condotta, la modifica o la proroga è conforme al regolamento o, nel caso di cui al paragrafo 3, fornisce adeguate garanzie, il comitato trasmette il suo parere alla Commissione. A questo punto la Commissione può decidere, mediante atti di esecuzione, che il codice di condotta, la modifica o la proroga approvati, che le sono stati sottoposti hanno validità generale all'interno dell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2 del regolamento.

La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 9 dell'art. 40 del GDPR.

Il comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

# *M4.6* – Sistemi informatici integrati e misure di sicurezza

## *Eliminare dati e tracce in modo sicuro – I parte*

***Dott. R. Grieco***

# Le tracce

# Dove si lasciano?

## 1. Localmente

Log; file cancellati, temporanei, swap

Cookies, cronologia, buffer, cache

Voci di registro

## 2. In rete

(~fuori controllo)

# Che cosa si lascia?

- password (!!)
- file riservati
- dati personali e sensibili
- cronistorie (navigazione, ultimi file aperti...)
- (...)

# pericolo: buttare i PC vecchi e rotti

(gli HD possono contenere di tutto)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008

**[1571514]**

---

- PC dismessi
- Stampanti multifunzione / fotocopiatrici a noleggio

# Come si cancella *seriamente*?

# *candidi tentativi*

1. cancellare il file
2. come 1, poi svuotare il cestino
3. come 2, poi scrivere qualcosa sull'hd
4. formattazione rapida
5. formattazione totale
6. formattazione e cambio delle partizioni

(10= lettura come file non cancellato, 0=impossibile recuperare)

# *candidi tentativi*

| | facilità di recupero |
|---|---|
| 1. cancellare il file | 9 |
| 2. come 1, poi svuotare il cestino | 9 |
| 3. come 2, poi scrivere qualcosa sull'hd | ~ |
| 4. formattazione rapida | 8 |
| 5. formattazione totale | 4 |
| 6. formattazione e cambio delle partizioni | 3 |

(10= lettura come file non cancellato, 0=impossibile recuperare)

# cancellazione di un file

l'operazione è stranamente veloce...

questo perchè il file **non** viene effettivamente cancellato, ma *marcato come cancellato*

e può essere recuperato facilmente

# Formattazione veloce

Si azzera solo l'indice del volume,

non viene cancellato nulla

# Come cancellare definitivamente

*o almeno provarci*

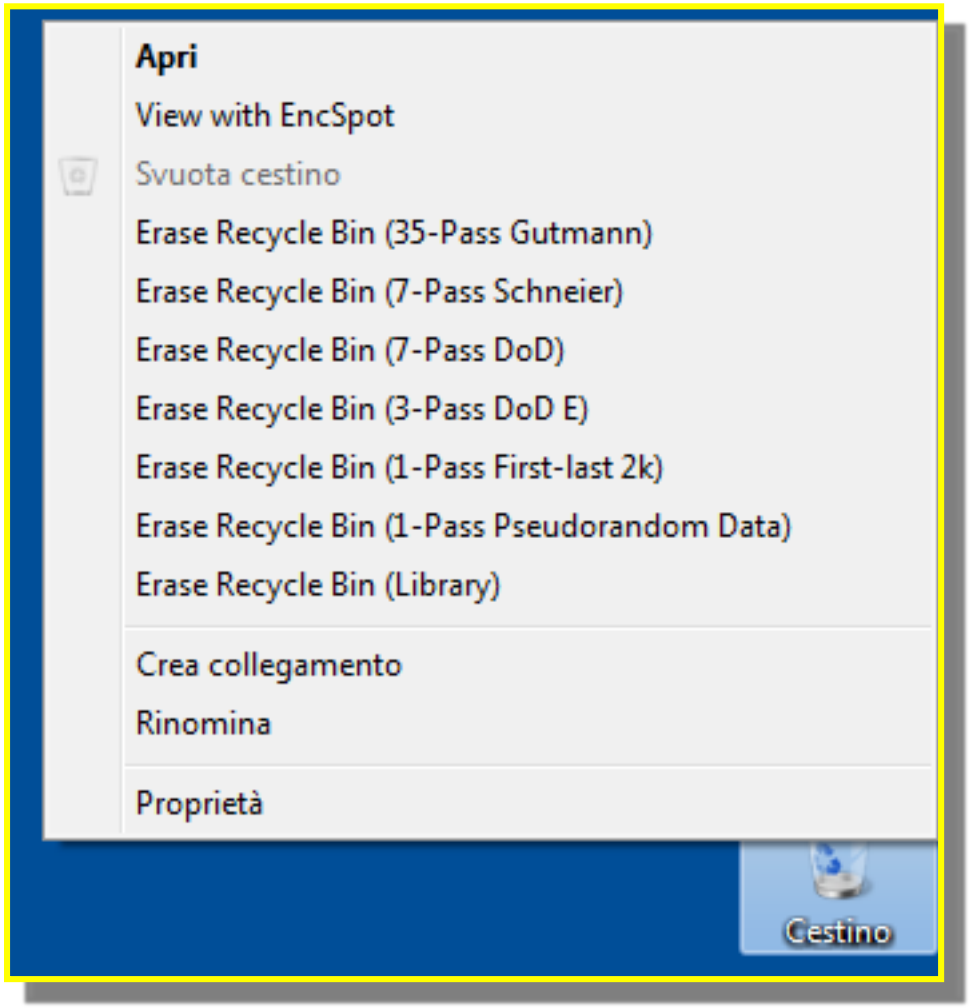
1. **File:** Eraser, ShredOS...
2. **spazio libero:** Eraser, H2TestW
3. **Cookies, cronologia, cache:** *browser*
4. **Swap file** (memoria virtuale): *flush*
5. **Registro:** *registry cleaners*


File Edit View History Bookmarks Tools Help
lifewire.com
https://www.lifewire.com/free-data-destruction-software-programs-2626174
Lifewire
Search
GO
BUY › SOFTWARE & APPS
40 Free Data Destruction Software Programs
Completely free disk wipe and hard drive eraser software utilities
Share
Pin
Email
PRINT

# 1. ERASER (free)

ERASER

https://eraser.heidi.ie/



# come cancellare

*(segue)*

2. Cookies, cronologia, cache:

   impostazioni privacy del browser
3. Swap file (memoria virtuale):

   flush (impostazione di windows)
4. Registro:

   *Eusing Registry cleaner*, *wise registry cleaner*...

# distruzione fisica

- trituratore
- calore
- degausser

# DATA LEAKS

I dati possono *uscire* dal PC nei modi più impensati e continuamente in evoluzione:

Dagli altoparlanti

Dal monitor

Con le vibrazioni dell'HD

Dalla presa di corrente

Per colpa dell'utonto (compresi agenti governativi)

# contromisure

- spegnere gli altoparlanti
- coprire la telecamera
- disattivare il microfono
- schermare il monitor e il PC (*Tempest*)
- UPS

- collegare il cervello e informarsi

# *M4.6* – Sistemi informatici integrati e misure di sicurezza

## *Eliminare dati e tracce in modo sicuro – II parte*

*Dott. R. Grieco*

# Come evitare di *lasciare* tracce

1. Sistemi operativi 'sicuri' (Qubes, Tails…)
2. Live-CD
3. PC-Stick
4. Cifratura totale

# 1. Sistemi operativi *sicuri*

QUBES OS

A REASONABLY SECURE OPERATING SYSTEM

## WHAT THE EXPERTS ARE SAYING

"If you're serious about security, Qubes OS is the best OS available today. It's what I use, and free."
— Edward Snowden, *whistleblower and privacy advocate*

"Happy thought of the day: An attacker who merely finds a browser bug can't listen to my microphone except when I've told Qubes to enable it."
— Daniel J. Bernstein, *mathematician, cryptologist, and computer scientist*

"When I use Qubes I feel like a god. Software thinks that it's in control, that it can do what it wants? It can't. I'm in control."
— Micah Lee, *Freedom of the Press Foundation, The Intercept*

"Donated a % of my consulting company's last year revenue to Qubes OS. I rely on it for all my work, and recommend it to clients too."
— Peter Todd, *Applied Cryptography Consultant*

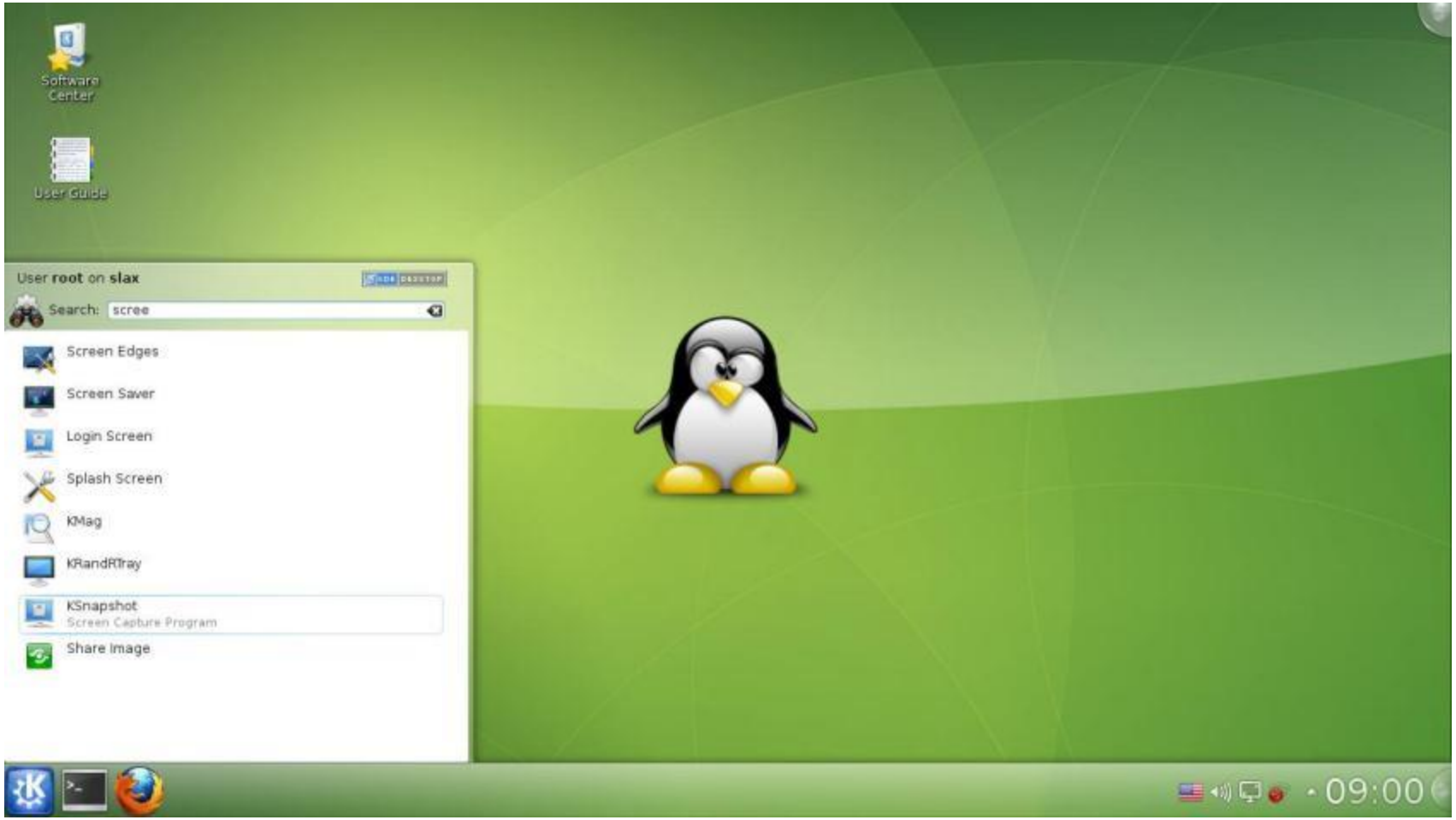
More From The Experts


Tails
LIVE OPERATING SYSTEM
ON A USB DRIVE


Tails
Privacy for anyone anywhere


About Tails
Tails
3.0
The Amnesic Incognito Live System
Build information:
3.0 - 20170610
efd101b1df3c21f5217b776d7735e129849b758a
live-build: 3.0.5+really+is+2.0.12-0.tails5
live-boot: 1:20170112
live-config: 5.20170112
Website
Tails developers
Credits
License
Close

# 2. Live-CD


Software Center
User Guide
User root on slax
Search: scree
Screen Edges
Screen Saver
Login Screen
Splash Screen
KMag
KRandRTray
KSnapshot
Screen Capture Program
Share Image
09:00

# 3. PC-Stick (compute stick)


Un PC-stick si connette direttamente al monitor

con una tastiera e un mouse (NON wireless!!) diventa un PC completo, isolato e ragionevolmente sicuro.

Basta non dimenticarselo...

# 4. Cifratura totale

*(modulo 4.2: cifratura di file, cartelle e volumi)*

i programmi usati possono essere gli stessi

# Cifratura totale

Cifratura del disco di sistema, dei dischi dati e di tutti i supporti portatili che si usano

*(in sintesi: non trattare mai dati in chiaro)*

Possibilità offerta da vari programmi di cifratura:

TrueCrypt, VeraCrypt,...

comprende la possibilità della *deniable plausibility*

# Cifratura totale

quando il disco di sistema è criptato, all'accensione viene chiesta la *passphrase* di cifratura.

qualsiasi cosa nel volume (disco o partizione) di sistema è visibile solo mentre il sistema sta funzionando

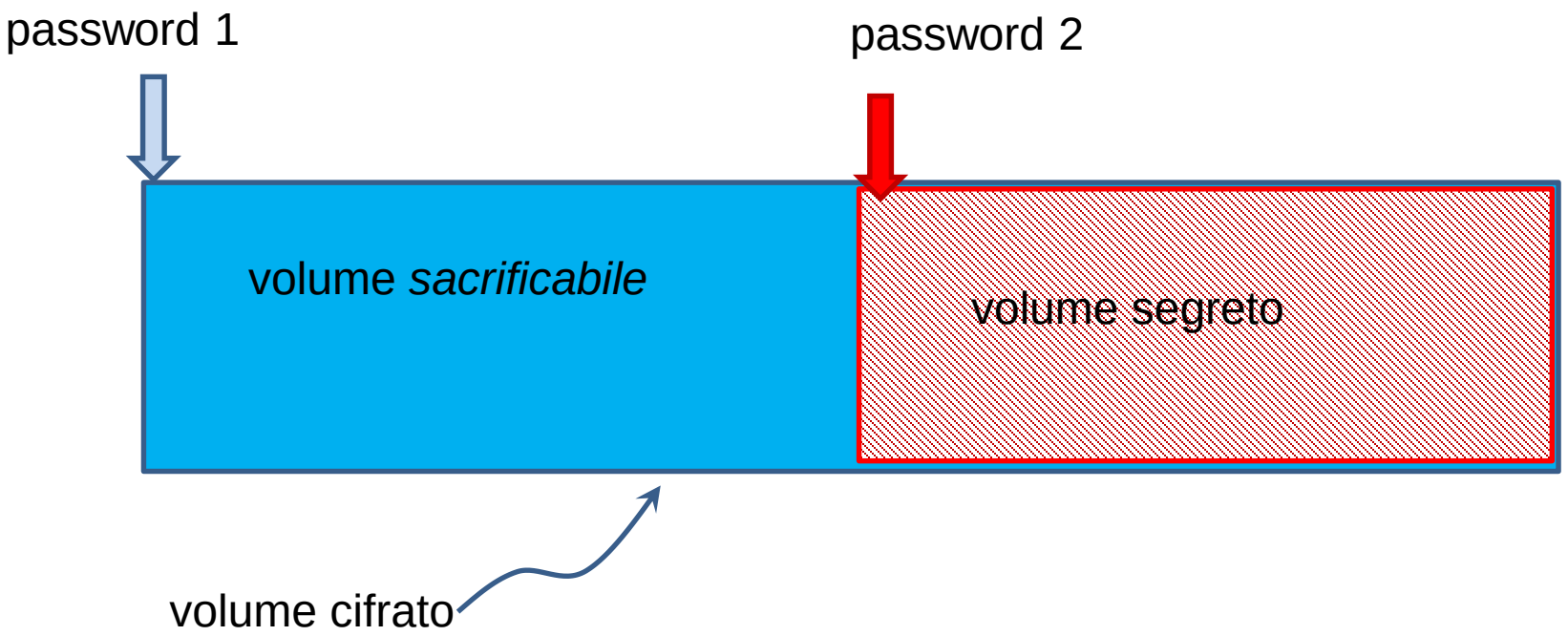
servono solo piccole attenzioni (RAM, rete, supporti esterni...)

si può fare in modo che tutti gli altri volumi vengano montati automaticamente alla partenza senza dover immettere altre password

e si possono far montare anche supporti esterni appena vengono collegati (HD, penne USB...)

# Cifratura totale

*deniable plausibility*



# IL COMPUTER SICURO (?)